DOCUMENT RESUME

ED 473 675 JC 030 118

TITLE	Protecting Information: The Role of Community Colleges in Cybersecurity Education. A Report from a Workshop Sponsored by the National Science Foundation and the American Association of Community Colleges (Washington, DC, June 26-28, 2002).
INSTITUTION	American Association of Community Colleges, Washington, DC.
SPONS AGENCY	National Science Foundation, Washington, DC.
PUB DATE	2002-06-26
NOTE	136p.
CONTRACT	DUE-0120666
AVAILABLE FROM	For full text: http://www.aacc.nche.edu/cybersecurity.
PUB TYPE	Collected Works - Proceedings (021) -- Reports - Descriptive (141)
EDRS PRICE	EDRS Price MF01/PC06 Plus Postage.
DESCRIPTORS	Community Colleges; *Computer Security; Computers; Crime; *Crime Prevention; *Information Science; Information Technology; Internet; Job Training; Law Enforcement; *Security Personnel; *Technical Education; Two Year Colleges; Vandalism; World Wide Web

ABSTRACT

The education and training of the cybersecurity workforce is an essential element in protecting the nation's computer and information systems. On June 26-28, 2002, the National Science Foundation supported a cybersecurity education workshop hosted by the American Association of Community Colleges. The goals of the workshop were to map out the role of the community college in this effort and to specify the community college's unique contribution to the preparation of cybersecurity professionals at all levels. The Computer Security Agency and the FBI issued an annual report on security trends and issues. Some of the issues confirmed by the 2002 report are: (1) organizations continue to be under cyber attack from both inside and outside their perimeters; (2) 74% of organizations cite their Internet connections as the most frequent points of attack, while 33% cite their internal systems as the points of attack; (3) 90% of all respondents had detected security breaches within the last 12 months; and (4) attacks occur despite a wide range of security technologies: 89% of respondents had firewalls, 82% had some sort of access control, and 38% used digital signatures. This report includes recommendations for integrating standards and certification into courses and programs, and for ensuring that cybersecurity professionals are qualified upon completion of programs. Appended are: Workshop Agenda; Keynote Speaker Bibliographies; Cybersecurity Education Resources; and a list of workshop participants. (Contains 163 references and resource contacts.) (Author/NB)

Reproductions supplied by EDRS are the best that can be made
from the original document.

Protecting Information

The Role of Community Colleges in Cybersecurity Education

ED 473 675

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
☑ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

TC030118

A Report from a Workshop
Sponsored by the National Science Foundation
and the American Association of Community Colleges

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY
D Carey
TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
1

BEST COPY AVAILABLE

Protecting Information

The Role of Community Colleges in Cybersecurity Education

A Report from a Workshop
Sponsored by the National Science Foundation
and the American Association of Community Colleges

June 26–28, 2002
Washington, D.C.

Community College Press®
a division of the American Association of Community Colleges
Washington, D.C.

This report is based upon work supported by the National Science Foundation under grant number DUE-0120666 to the American Association of Community Colleges.

The American Association of Community Colleges is the primary advocacy organization for the nation's community colleges. The association represents 1,100 two-year, associate degree–granting institutions and some 10 million students. AACC provides leadership and service in five key areas: policy initiatives, advocacy, research, education services, and coordination/networking.

The National Science Foundation (NSF) is an independent agency of the U.S. Government whose mission is to promote the progress of science; to advance the national health, prosperity, and welfare; and to secure the national defense. The foundation competitively awards grants for research and education in the science, technology, engineering, and mathematics fields.

© 2002 American Association of Community Colleges. Photocopying for nonprofit educational purposes is permitted. This report is also available online at www.aacc.nche.edu/cybersecurity.

Community College Press
American Association of Community Colleges
One Dupont Circle, NW
Suite 410
Washington, DC 20036-1176
Fax: (202) 223-9390

Printed in the United States of America.

Contents

Foreword v
Introduction 1
Executive Summary 5

Recommendations

1. The Role of Certifications and Skill Standards 9
2. Establishing and Maintaining Cybersecurity Programs at Community Colleges 13
3. Topics, Courses, Curricula and Programs 19
4. Preparation for Cybersecurity Positions 27
5. Advancing the Role of Community Colleges in Cybersecurity Education: Recommendations to Stakeholders 31

White Papers

6. Case Study: Creation of a Degree Program in Computer Security 39
7. Cybersecurity Education in Community Colleges Across America: A Survey of Present and Planned Implementation 57
8. IT Security Specialist—Integrating Academic Credentials with Professional Certifications 73
9. Adapting Commercial Training Materials for Use at the Community College 89
10. Trustworthy Computing 101

Appendixes

Workshop Agenda 115
Keynote Speaker Biographies 119
Cybersecurity Education Resources 121
Workshop Participants 129

BEST COPY AVAILABLE

Foreword

The issue of national security and the need to protect the nation's information systems, networks, and infrastructures could not be more prevalent. President Bush recently directed the development of a *National Strategy to Secure Cyberspace* to ensure that America has a clear roadmap to protect its important infrastructures that could be vulnerable to cyber attacks. In conjunction with this national call to secure cyberspace, leaders of higher education have worked to identify strategies and resources to help meet the nation's educational and workforce needs in this critical high-tech area.

In June 2002, the National Science Foundation (NSF) and the American Association of Community Colleges (AACC) cosponsored a workshop on "The Role of Community Colleges in Cybersecurity Education." Over 90 experts in computer, network, and information security from community colleges, four-year institutions, business, industry, and government convened to focus on how community college resources could be utilized and further developed to help educate a cybersecurity workforce.

The workshop was developed with leadership from a steering committee and the National Science Foundation's Division of Undergraduate Education, with significant support from other divisions in the Directorate for Education and Human Resources. AACC is grateful to the steering committee and the National Science Foundation for their important role in working toward providing innovative opportunities for community college students, preparing cybersecurity technicians, and securing our national defense.

This report focuses on the key findings and recommendations from "The Role of Community Colleges in Cybersecurity Education" workshop. It is one of several activities supported by an NSF grant to the American Association of Community Colleges. We thank the foundation for its continued support of community colleges and their students.

George R. Boggs
President
American Association of Community Colleges

BEST COPY AVAILABLE

Introduction

Computers are rarely found in isolation. They are connected with one another through local area networks, wide area networks, and the Internet. This connectedness has made the security of computers and information a major challenge. People who use computers and the Web increasingly encounter viruses and worms, the theft of personal information, software that monitors their Web-surfing habits, and defaced Web sites. Network administrators spend more and more time preventing, detecting, and investigating intrusions and security lapses of various sorts. Law enforcement officials at all levels are having to redirect resources to combat the proliferation of computer crime.

The Computer Security Institute's 2002 Computer Crime and Security Survey[1] of large corporations and government agencies revealed that

- 90 percent of respondents had detected computer security breaches;
- 80 percent of respondents had suffered financial losses as a result of computer breaches;
- 85 percent of respondents had detected computer viruses; and
- 78 percent of respondents had detected employees' abuse of Internet access privileges (e.g., downloading pornography or pirated software, or inappropriate use of e-mail systems).

In addition, 75 percent of respondents cited their Internet connection as a frequent point of attack, and 33 percent cited their internal systems as a frequent point of attack. In 2001, Carnegie Mellon University's Computer Emergency Response Team (CERT) Coordination Center handled 52,658 computer security incident reports, more than twice the number handled during the previous year.[2]

Reliable, secure information systems underpin not only government operations but also the functioning of key industries that hold the nation together economically and socially. Executive orders in both the Clinton administration and the current Bush administration established government leadership efforts to protect the information systems that support the nation's critical infrastructure—telecommunications, transportation, energy, health care, banking and financial services, emergency services, manufacturing, and water supply systems. The events of September 11, 2001, only deepened long-standing concerns about the nation's information systems and communications networks' vulnerability to terrorism and other disruptions.

[1] Richard Power, "2002 CSI/FBI Computer Crime and Security Survey." *Computer Security Issues and Trends*, vol. 8, no. 1 (Spring 2002). Available online at www.gocsi.com.

[2] See www.cert.org/stats/cert_stats.htm.

The private sector and government have found it difficult to fill information technology jobs with qualified workers. Potential cybersecurity threats create an additional need for an expanded technical workforce with appropriate, specific knowledge and skills. All computer users need to be aware of the basic aspects of computer security so that they can protect themselves at home and in the workplace. The challenge of providing specialized training for computer experts and basic computer security training for all U.S. citizens extends to institutions at all levels of the formal educational system, including those that provide supplementary training for people who are already in the workforce.

The National Science Foundation (NSF), a major federal funder of research and education in computer-related fields, is well positioned to catalyze educational activities in computer and network security. NSF's Federal Cyber Service: Scholarship for Service (SFS) program,[3] which focuses on university-level education in information assurance and computer security, is one of five Federal Cyber Service training and education initiatives aimed at strengthening the nation's cybersecurity workforce, especially the federal workforce that secures the government's information infrastructure. The program provides grants to institutions that the National Security Agency (NSA) recognizes as Centers for Academic Excellence in Information Assurance Education (and to institutions that have equivalent programs) to award full scholarships to undergraduate or graduate students who are in their final two years of study. In return for the scholarships, the students must take cybersecurity positions in the federal government for two years after they graduate. The program also supports faculty development activities to improve and spread instructional capability in information assurance and computer security.

Technical education about cybersecurity issues is needed for employment in a wide range of fields, including software engineering, network administration, banking, e-business, and law enforcement. The relevant occupations cover a vast spectrum of knowledge and skills. Part of this spectrum (which could account for a significant share of the workforce demand) can be effectively addressed by courses and programs at community colleges. Because many positions in the broad cybersecurity arena can be filled by workers who hold two-year degrees or who obtain relevant certification, and because many students who begin their technical education in two-year colleges transfer to four-year programs, it is natural for NSF to look at community colleges as a focus for cybersecurity program development.

Since 1994, NSF's Advanced Technological Education (ATE) program[4] has provided grants to improve the education of technicians, especially students in community college programs, in the high-tech fields (information technology, biotechnology, manufacturing, etc.) that drive the U.S. economy. This workforce-oriented program focuses on the needs of employers and stresses partnerships between community colleges, four-year colleges and universities, secondary schools, business, industry, and government. The ATE program has a large number of active grants in information technology, including two national centers (in Washington State and Florida) and two regional centers (in Kentucky and Nebraska) that conduct

[3] The Web address for the SFS program can be found in the Cybersecurity Education Resources Section of this report.

[4] The Web address for the ATE program can be found in the Cybersecurity Education Resources Section of this report.

comprehensive educational activities, as well as about 30 information technology projects with a narrower focus. These centers and projects educate students and provide professional development for faculty in network administration, database administration, Web development, e-commerce, personal computer hardware and operating systems, and other topics required for entry-level employment in information technology.

Information technology specialists and telecommunications technicians, including those educated through ATE-funded centers and projects, confront threats to computer, information, and Internet security and contribute to intelligence gathering and law enforcement. These professionals are part of the cadre of foot soldiers who are on the front lines of cybersecurity defense, protecting the information assets of business, industry, and government.

Community colleges are well suited for educating information technology professionals in cybersecurity. Community colleges serve the workforce needs of their regions. They can respond quickly to put new programs in place. They have close ties with business and industry and work with business and industry professionals to develop curricula. Community colleges serve first-time students as well as returning students and workers who are seeking new career opportunities or new skills to keep them employable in a changing economy. They provide the first entrance to higher education for most minorities and first-generation college students, and they give students a pathway to higher education.

Community colleges offer not only degree programs but also courses that lead to certification in various information technology subjects. Industry-endorsed and vendor-specific certification is important to employment in a number of information technology occupations, and workers who already hold two-year or four-year (or higher) degrees often seek such certification. Such certification, whether it is in addition to or in place of a degree, is likely to take on increasing importance for employment in cybersecurity-related occupations. Community colleges are well positioned to offer the training that leads to such certification. Indeed, they already do so, with such courses being part of many associate degree curricula.

The American Association of Community Colleges (AACC), which represents more than 1,100 associate degree–granting institutions, has strongly supported the ATE program and NSF's other efforts to improve science, mathematics, engineering, and technology education at community colleges. AACC joined with NSF in organizing the workshop that led to this report. Held on June 26–28, 2002, the workshop brought together nearly 100 experts in computer, network, and information security from community colleges, four-year colleges and universities, business, industry, and government (local, state, and federal) to consider how community college resources can be harnessed and expanded to help meet the nation's educational and workforce needs in cybersecurity.

Workshop participants explored a number of key questions, including the following:

- What cybersecurity jobs could be filled by people with an appropriate two-year degree or certificate, and what knowledge and skills are needed for those jobs?

- What relevant courses and programs already exist at community colleges, and what courses and programs need to be developed as models?
- What is the proper role of skill standards and professional certifications in education for cybersecurity occupations?
- What role can community colleges play in retraining current workers in aspects of cybersecurity?
- What connections should be made between community college programs and university programs in computer science and information assurance?
- What partnerships should community colleges forge with business and industry in order to build appropriate programs?
- What resources would enable and encourage community colleges to broaden their offerings in information technology, forensic science, and other subjects to address cybersecurity workforce needs?

This report details the workshop's agenda and conclusions, including specific recommendations for action by educational institutions, business, industry, government, and other stakeholders to improve cybersecurity education and build the cybersecurity workforce.

Executive Summary

The education and training of the cybersecurity workforce is an essential element in protecting the nation's computer and information systems. On June 26–28, 2002, the National Science Foundation (NSF) supported a cybersecurity education workshop hosted by the American Association of Community Colleges (AACC). The goals of the workshop were to map out the role of the community college in this effort and to specify the institution's unique contribution to the preparation of cybersecurity professionals at all levels.

Representatives from the nation's cybersecurity education programs addressed five overarching issues: skill standards and certification; cybersecurity programs at community colleges; specification of topics, courses, curricula, and programs; preparation for cybersecurity positions; and advancing the role of community colleges in cybersecurity education. Discussions crystallized the issues and shaped the five position papers presented in this report.

The Role of Certification and Skill Standards

Skills standards recommend foundational elements for programs and provide a set of core competencies. They can help define the field, provide uniformity across institutions, map programs to specific jobs, and provide guidelines that assist educational programs in evolving and adapting to changes in the field and in job requirements.

Certification can be an assessment of an applicant's qualifications as measured by performance on a standardized test, a mechanism for establishing articulation agreements between and among institutions, a way to encourage the formation of education/business/industry partnerships, and a system for continuing ongoing professional development and lifelong learning.

Recommendations: Participants identified key areas that require immediate and sustained activity:

- Creating collaborative initiatives to establish qualifications for cybersecurity professionals and to assist in local articulation agreements between and among programs and institutions.
- Integrating standards and certification requirements into courses and programs.
- Ensuring that cybersecurity professionals are qualified upon completing the program and entering the workforce or going on to other education programs.

- Providing resources and support for remaining at the forefront of the field.

Establishing and Maintaining a Cybersecurity Program at a Community College

Establishing and maintaining a cybersecurity program will require initial and ongoing investment. Collaboration between two-year and four-year institutions of higher education and business, industry, and government entities at all levels can help secure the resources needed to meet the demand for a high-quality cybersecurity workforce. These include high-quality educational materials and curricula, dedicated and state-of-the-art facilities, access to educational and training opportunities through diverse modes of instructional delivery systems, continuous opportunities for professional development and enhancement, and student recruitment and support systems.

Recommendations: Seven key elements need to be in place to support activities designed to establish and maintain cybersecurity programs at community colleges:

- Strong partnerships between two-year and four-year colleges and universities and business, industry, and government entities for generating revenue and for developing local articulation policy and procedures.
- Recognition and support systems for rewarding faculty and staff who contribute to the education and training of the cybersecurity workforce.
- Local and state government financial support and cooperation in the program approval process.
- Vendor and manufacturer donations for professional development and skill enhancement.
- Support from foundations and professional societies.
- Industry and business sponsorships of faculty and students.
- Program support from federal agencies.

Specification of Topics, Courses, Curricula, and Programs

Community colleges prepare a wide range of cybersecurity professionals. Two-year institutions train entry-level workers, provide workers with opportunities to maintain high levels of skills and knowledge, serve workers who are trying to change jobs or positions, and prepare students for transfer to four-year programs. To navigate this diversity, students need to have a clear understanding of their options and responsibilities, and of the goals of the programs in which they are enrolled. The workshop participants developed a framework of six core areas for specifying topics, courses, curricula, and programs and linking them to hands-on real-world activities. The six core areas are security issues; business and economic issues and security policies; law, ethics, and standards; general knowledge and skills; Inter-

net and cybersecurity skills and knowledge; and knowledge of industry hiring practices in cybersecurity.

Recommendations: Specification can provide guidelines that increase the following:

- Preparation of students for immediate employment and continued career advancement.
- Alignment and adaptability of content, with a focus on outcomes.
- Student support and advising systems.

Preparation for Cybersecurity Positions

Participants agreed that many existing jobs in cybersecurity can be filled by people with two-year degrees. A two-year degree can serve as a prerequisite for many industry-endorsed certifications, can be combined with a liberal arts or technology-oriented bachelor's degree, and can be used as a basis for continuing education and training.

Recommendations: To prepare different segments of the workforce for cybersecurity positions, stakeholders should

- Use the National Security Agency categorization of security positions as a framework for developing program requirements.
- Develop collaborative activities across institutions to promote careers in cybersecurity.
- Encourage students to participate in cocurricular activities that are attractive to future employers and graduate schools.
- Pressure government agencies to provide descriptions of cybersecurity positions and guidelines for salaries.

Advancing the Role of Community Colleges in Cybersecurity Education

Participants agreed that all stakeholders have a responsibility for advancing the role of community colleges in cybersecurity education and training. Stakeholders include community colleges; four-year colleges and universities; business and industry; professional and trade associations; and local, state, and federal government entities, including the National Science Foundation.

Recommendations: The responsibility for cybersecurity is broad based. Table 1 presents the essential responsibilities of each stakeholder in this endeavor.

Table 1. Essential Responsibilities of Cybersecurity Education Stakeholders

	Two-Year and Four-Year Partnerships	Community Colleges	Four-Year Colleges	Business and Industry	Professional and Trade Associations	Local, State, and Federal Government
Form close collaborations	●	●	●	●	●	●
Ensure and promote student success	●	●	●	●	●	●
Support program development and implementation	●					●
Facilitate coordination and articulation of programs and courses	●		●			
Take a broad-based approach to curriculum development, design, and delivery	●	●	●			
Ensure that faculty in two-year and four-year institutions are well prepared		●	●	●	●	●
Encourage cybersecurity professionals to share their expertise				●	●	●
Provide service to the community	●					
Market programs to the community	●	●		●	●	●
Find and utilize resources	●	●	●			

BEST COPY AVAILABLE

1. The Role of Certifications and Skill Standards

Five breakout groups at the workshop discussed the role of skill standards and certifications in cybersecurity. The issues listed below were provided to the participants for discussion; most of the discussions focused on the first two. Participants agreed that a distinction should be made between skill standards and certifications:

- Skill standards recommend foundational elements for programs and provide guidance on the competencies that are needed for people to perform jobs.
- Certifications are a validation of credentials and skills.

In addition to the skills measured on a test, a certification may require one to have work experience before being allowed to take the test or work experience to earn the certification. The certification process should not drive curriculum development, because certification is not an end in itself but a starting point for many careers. Certifications do, however, serve many useful purposes, as described below. See "Cybersecurity Education Resources" on page 121 for a list of some certifications in cybersecurity that workshop participants identified.

Issues

1. What is the proper role of certifications and skill standards?
2. What are the strengths of existing certifications and skill standards?
3. What are the gaps in existing certifications and skill standards?
4. What are the relative merits of vendor-neutral and vendor-specific certifications?
5. In addition to written tests, what other validation is needed?
6. How can an institution be confident that faculty are not just teaching to a test?
7. Is cybersecurity a specialization, or should it be embedded across the information technology (IT) curriculum?

Strengths of Certifications and Skill Standards

Certifications can be used for

1. **Validation.** They
   - Establish a baseline for what people know or don't know.
   - Reliably indicate a person's possession of certain skills according to objective criteria.
   - Establish a credibility that extends outside a particular organization.
2. **Marketing** to help sell a program to students and to industry.
3. **Delegating** authority in the hiring process, because many people who evaluate applicants for a position may not know all the skills needed for it. Certifications provide a convenient indicator of whether people know what they are supposed to know to do a particular job. Companies and hiring officials trust a certification authority to say that an individual is skilled at a certain level.
4. **Career progression.** Certifications
   - Are usually recognized outside the college.
   - Are often progressive and allow people to build on the knowledge and skills that they have.
   - Help students move between academic institutions and from academic institutions to business and industry.
5. **Program development,** because
   - Curricula associated with certifications may help establish a program.
   - Certifications offer industry validation of skills and help educational institutions provide students with the skills and knowledge that industry and associations think they should have.
   - Certifications encourage academic institutions and business and industry to work together to develop programs that can help students move between organizations.
   - Certifications can be incorporated into academic programs as an objective of some classes and provide added value to classes and degree programs.

Skill Standards can be used to

1. Help define the field.
2. Sell a program that is built on skill standards.
3. Set up a program.
4. Recommend curricula.
5. Provide uniformity across institutions.
6. Establish a common terminology.
7. Map programs to specific jobs.
8. Help programs evolve and adapt as the field changes.

Recommendations

1. **Cybersecurity certifications should**
   a. Be developed to
      - Help colleges work together to provide educational certifications that articulate among institutions. These certifications might be used between colleges or between colleges and the workplace.
      - Build collaborations between academia and industry based on realities of current technologies.
      - Offer progressive levels of certification, depending on the level of particular jobs.
      - Benchmark practitioners and provide a starting point for assembling basic skills.

   b. Be incorporated into academic programs in community colleges to
      - Be part of the objectives of many classes.
      - Allow students to see real applications while learning general skills.
      - Ensure that the institutions prepare students in general skills and knowledge, but also prepare them to sit for exams if they desire.
      - Be vendor neutral for general courses, but ensure that students can take and pass vendor-specific examinations when needed.

   c. Ensure that students can do more than just pass a test. Certifications often ask a person to exhibit knowledge, but a demonstration of applications is also needed.

2. **Cybersecurity Skills Standards should**
   a. Build on standards that already exist. Many standards have already been developed and can be used and adapted to community college programs.
   b. Provide a balance between specific technical skills and the broader skills needed for lifelong learning.
   c. Incorporate hands-on preparation in addition to theoretical understanding so students learn *how* to do something and *why*.
   d. Complement certifications and degrees.
   e. Be developed by many different organizations.

> Even in today's difficult economy, the demand for cybersecurity professionals is outstripping supply. High-tech companies and government agencies are using innovative programs to recruit and train workers with specialized skills in information security. America needs educational programs to prepare the IT workers of the future to maintain the security of our systems, and that is where community colleges come into the picture.
>
> —George R. Boggs, President and CEO, American Association of Community Colleges

f. Provide suggestions for students who wish to enter the workplace as technicians, transfer to a four-year program, or be retrained in cybersecurity as a specialty.
g. Include understanding of the judicial system, including investigative processes, chain of evidence, and incident reporting.
h. Promote standardization and consistency among organizations.
i. Encourage performance-based testing.
j. Suggest ways to evaluate recommended skill sets.

2. Establishing and Maintaining Cybersecurity Programs at Community Colleges

Workshop participants were asked to address five issues related to establishing and maintaining cybersecurity programs at community colleges.

Setting up and maintaining such programs requires an initial financial investment as well as an ongoing obligation to provide resources. Partners in business, industry, and government are needed to help develop programs and market them to the community. Partners can provide resources such as computers, laboratory space, curricula, materials, internships for students, externships for faculty, scholarships, and people to serve on curriculum and advisory committees.

Issues

1. What resources are needed to establish and maintain a cybersecurity program?
2. How can faculty be prepared to teach in this field?
3. What partnerships with business, industry, and government should be developed?
4. What components of a college's existing computer and information technology programs can serve as the basis for a cybersecurity program?
5. How can a college obtain the resources needed to start and maintain a cybersecurity program?

Resources Needed to Start a Program

1. **Partners and Administrative Support**
   - Analysis of needs.
   - Partnerships with business, industry, and government.
   - Partnerships and articulation agreements with four-year colleges and universities and local high schools.
   - Commitment from high-level administrators.
   - State approval and funding.

2. **Educational Materials and Curricula**
   - Fast-track for curriculum and program approval.
   - Textbooks and materials.
   - Frameworks for curricula.
   - A cybersecurity clearinghouse Web site with links to community colleges that have or are developing cybersecurity programs, and other materials and resources.
   - Core materials for adjunct faculty.
   - Provisions for advanced certificates and an associate degree.
   - Alternative delivery models such as distance learning, flexible scheduling, and modular curricula to meet the needs of a variety of students.
   - Continuing education options.
   - Vendors to give technical demonstrations of materials and equipment.

3. **Physical Resources**
   - Dedicated laboratories and classrooms that are electronically isolated.
   - A laboratory to mimic the environment and real components of industry.
   - Periodic updating of laboratories.
   - A collection of legacy hardware and software, because both new and old systems get attacked.
   - Multiple operating systems and swappable hard drives.
   - A place to store equipment securely.
   - Course management systems such as Blackboard, WebCT, and Prometheus.

4. **Staff Resources**
   - Support to prepare existing faculty in computer technology, information technology, and other programs to teach cybersecurity topics and courses, to help them develop new programs, and to help them become certified.
   - Cooperation with a local university so that faculty can get graduate credit for cybersecurity courses.
   - Continuing education for faculty who hold certifications to ensure that they remain current.
   - Faculty recognition and rewards for further education and training.
   - Faculty participation in professional organizations relating to security, such as the Information Systems Security Association (ISSA), Infragard, and the Information Systems Audit and Control Association (ISACA).
   - Effective use of local experts from business, industry, and government as adjunct instructors and guest speakers.
   - Faculty participation in vendor training.
   - Inservice teacher training for adjuncts (for example, how to prepare for classes, how to evaluate students, and what to expect from students).
   - Supervision of adjunct faculty.

- Knowledge management to maintain core knowledge within the institution in the face of faculty turnover.
- Creative ways to attract highly qualified full-time faculty, including those from unconventional groups (for example, people who are ready for a change of jobs, IT professionals who are tired of 24/7 intensity, retired people who want to keep current, people who have family commitments).
- Faculty and staff internships and externships.
- Mentoring programs to coach new faculty.
- Differential pay scale for cybersecurity faculty (full- and part-time).
- National networks of instructors who can exchange information.
- Links between educators and scientists and engineers.
- Sabbaticals for faculty.
- Scholarships from industry for faculty to participate in conferences.

5. **Student Preparation**
   - Prerequisite body of knowledge.
   - Faculty advisors to make sure students are properly placed.
   - Internships to help prepare students to work in industry.
   - Student membership in professional organizations.
   - Practice certification exams.
   - Technical writing and communication skills.
   - Understanding that the world of cybersecurity will change and that students need to develop lifelong learning skills in order to be able to change with it.

6. **Marketing of Programs**
   - Proactive involvement of community college faculty in campaigns to attract students to cybersecurity programs, including visits to secondary schools and employers.
   - Well-prepared counselors who know how to advise students about cybersecurity careers and programs.
   - Knowledge of what attracts students to cybersecurity courses and programs.
   - Industry and government support for workers to take cybersecurity courses and programs.

Resources Needed to Maintain an Established Program

The workshop participants felt that the resources needed to start a program would also be needed to maintain a program. In addition, they recommended additional resources related to the following:

1. **Faculty**
   - Campus or local chapters of the American Society for Industrial Security (ASIS) and other national organizations.
   - Funding for faculty development, internships, and sabbaticals.
   - Funds for faculty to attend industry and professional society meetings.
   - National workshops and regional events in cybersecurity for faculty and administrators to learn about programs, materials, and other resources.

2. **Students**
   - Continuing professional development options to help program graduates maintain skills and advance in their careers.
   - Campus or local chapters of ASIS and other national organizations.
   - Employment of current students as mentors for incoming students.

3. **Courses and Programs**
   - Continuous funding for programs and courses.
   - Funding for upgrading and adding equipment and software.
   - Laboratory or equipment fees from students.
   - Streamlined process for updating curricula.
   - Relationships with industry, government, and other institutions to build expertise and networks.

4. **Marketing and Attracting Students to Programs**
   - Recognition of the associate degree and certifications as appropriate credentials for certain cybersecurity jobs.
   - Building alumni relationships.
   - Advertising and marketing programs and new course offerings.
   - Business, government, and industry support of programs for their own workers.
   - Outreach to high schools, including using current college students as ambassadors to high schools.
   - Short workshops to expose high school students to cybersecurity careers.
   - Special on-campus lectures and seminars cosponsored by groups like Infragard.

Securing Necessary Resources

1. **Partnerships should be established between two- and four-year colleges, business, industry, and government to**
   - Develop educational materials, courses, and programs that fit their needs.
   - Use industry expertise to help develop curricula or program modules.
   - Involve practitioners as well as managers.

- Share equipment (such as a centralized server that could be used by many partner institutions).
- Share the knowledge base.
- Share faculty between two- and four-year institutions.
- Have graduate students teach in programs and mentor students in community colleges.
- Seek program support from government agencies, business and industry, and other sources.
- Influence policy to ensure that cybersecurity programs get support.
- Work with local chapters of various cybersecurity organizations, such as the Information Systems Security Association (ISSA) and the High Technology Crime Investigation Association (HTCIA).
- Work with local economic development organizations.

2. **College and university administrators should**
   - Be approached for support through demonstrations of the relevance of and need for the programs.
   - Develop partnerships with large industries (such as insurance, health care, and banking and other finance) that are big consumers of technology and deal with cybersecurity issues on a daily basis.
   - Encourage faculty to apply for state and federal funding.
   - Encourage faculty participation in associations such as the Society for Information Management (SIM) and Colloquium for Information Systems Security Education (CISSE).
   - Try to influence policies to make sure resources are available.
   - Support alternative delivery models for programs, such as shorter courses, flexible scheduling models, "burst mode" instruction, and modular curricula.
   - Allow IT programs to keep their own laboratory fees instead of contributing them to the collegewide pool.

3. **State and local governments may provide**
   - Money tied to homeland security issues, infrastructure support, and incident response.
   - Fast-track approval of curricula and programs.

> **"In this changing world, national security no longer means defense in its traditional form, and sharp distinctions between foreign and domestic threats no longer apply. Security must now encompass 'economics, technology, and education for a new age in which novel opportunities and challenges coexist uncertainly with familiar ones.'**
>
> —Judith A. Ramaley, Assistant Director, Directorate for Education and Human Resources, National Science Foundation

4. **Vendors and manufacturers can**
   - Donate resources such as free or substantially discounted software, computers, networking equipment, educational materials, etc.
   - Provide memberships in professional societies for faculty and students.
   - Offer training for faculty prior to or coinciding with the release of new operating systems, hardware, etc.
   - Include faculty in vendor or industry training classes.

5. **Foundations and professional societies can**
   - Provide resources for programs.
   - Provide a network of support for faculty and students.
   - Supply letters of support or commitment for projects.
   - Serve as a liaison with business and industry.
   - Provide workshops and professional development opportunities for faculty.
   - Encourage faculty and students to attend meetings as both participants and presenters.
   - Encourage vendors to create and maintain partnerships with educational institutions.
   - Help faculty become aware of resources and grants that are available from a range of sources (state, federal, private, nonprofit, etc.).

6. **Industry can**
   - Support paid faculty externships and student internships (including faculty-student pairs).
   - Provide opportunities for job shadowing.
   - Encourage and provide time and resources for industry professionals to serve on advisory committees, teach as adjunct faculty, and work on curriculum and program improvement.
   - Loan or donate equipment to educational institutions.
   - Market programs to their own workers and the community.
   - Try to influence policies to make sure resources are available.

7. **Federal agencies such as the National Science Foundation (NSF) and the National Security Agency (NSA) should**
   - Have programs that support the development and improvement of cybersecurity programs.
   - Recognize the role that community colleges can play in educating students for cybersecurity careers.
   - Support the development of Web-based learning tools.
   - Support workshops and meetings for all cybersecurity stakeholders to interact.
   - Create or support a Web site where educators can post cybersecurity course materials and other educational materials.
   - Provide speakers, adjunct faculty, internships for students, externships for faculty, members for advisory boards and curriculum committees, and workers to help develop instructional materials and programs.

3. Topics, Courses, Curricula and Programs

The workshop participants agreed that community colleges have multiple roles in cybersecurity education. The colleges can prepare both cybersecurity generalists and specialists. Community colleges

- Prepare entry-level workers—those who have little or no work experience—to go to work.
- Provide lifelong learning to ensure that workers maintain a high level of skills and knowledge. These people have work experience and may or may not already have two- or four-year degrees.
- Serve workers who are trying to change jobs or positions. These people may be trying to get into a new field, increase their upward mobility in their companies, or upgrade the skills used in their current positions.
- Prepare students to transfer to four-year programs.

It may be difficult for a single program at a community college to satisfy all four types of students. Students should clearly understand what options programs offer and understand the purpose and goals of the programs in which they are enrolled.

Fundamentals of computer security and information assurance need to be further defined because no common definitions of skills and terms exist. Curricula are changed and modified frequently, often based on market demands, but market demand–driven programs can be narrowly focused and not serve students broadly. Workshop participants discussed the following issues:

Issues

1. What topics should be incorporated into all cybersecurity programs?
2. What and how many cybersecurity topics should be embedded in other computer programs?
3. Can the topics be packaged into a general survey course?
4. Where will the course materials come from?

5. Can two-year and four-year programs in cybersecurity be aligned so that students completing a two-year program can transfer to a four-year program?
6. If a student in a two-year technician program decides to transfer into a four-year program, what additional courses will he or she need to take? If a student enters a two-year program wanting to prepare to be a technician, are there courses that he or she could take that would keep pathways to four-year programs open?
7. What are the proper degrees and credentials for faculty in cybersecurity programs? Are both academic and professional qualifications required?
8. How will accrediting rules affect cybersecurity programs?

Topics

Several workshop groups recommended that a cybersecurity program include a general survey course that covers a wide range of topics, such as systems design and analysis, databases, business skills, and behavior and communications skills. This course could be taken before students take more specific courses. It might be followed by a course where students look at the security of the institution and its vulnerabilities and make a presentation to the administration.

The recommended topics are grouped together for ease in reading, but are not necessarily independent or designed to be taught in separate courses. Topics in the general security issues area and the section on law, standards, and ethics could be taught in a survey course and integrated into computer and information technology programs as well as other programs across the college, including law enforcement, criminal justice, and business. The topics in the section on creating a business plan and reducing risk and vulnerability are more specific, but could be appropriate to specific cybersecurity programs, computer and information technology programs, and business and management programs. Specific cybersecurity topics are appropriate for students who seek a degree or a specialization in cybersecurity. The list is not meant to be exhaustive, but to provide a framework for developing courses and programs. The courses and programs a community college offers will vary depending on the needs of local employers.

Topics listed in the general, business, and law sections, when taught more deeply, also belong in the specific cybersecurity skills section. Workshop participants recommended that topics be introduced in earlier courses and then revisited in courses related specifically to cybersecurity jobs and degrees—students won't always "get it" the first time. Topics need to be revisited many times and continually used in subsequent courses. Fundamentals should be refined in a hands-on, real-world, but safe and controlled environment.

1. **General Security Issues**
   - Survey of computer security literacy issues, awareness, and ethics.
   - Knowledge of what resources should be protected.
   - User's best practices.
   - Host security.
   - Scope of security in relation to today's technologies.
   - Need for security policies.
   - Terminology.
   - Confidentiality, integrity, availability, authentication, authorization, and nonrepudiation.
   - Personal and corporate privacy issues.
   - The need to understand the unknown.
   - TCP/IP (Transmission Control Protocol/Internet Protocol). Workshop participants said that students must understand TCP/IP before they can successfully learn about cybersecurity.

2. **Business and Economic Issues and Security Policies**
   - Economic impact and planning.
   - Business-based security, including knowing users and clients.
   - Business and institutional structures, strategies, and policies.
   - Working with a business response team. Cybersecurity is only one element of the whole business plan.
   - Understanding that security is integral to an organization, not a stand-alone policy.
   - Knowing what a security policy is.
   - Policy, standards, and guidelines (such as for acceptable use, methods, and procedures).
   - Appropriate use policies.
   - Compliance procedures.
   - Vulnerability, threats, acceptable risk, and risk mitigation (including knowledge of an established taxonomy and an established trusted system for evaluation like the Information Technology Security Evaluation Criteria (ITSEC)).
   - Risk-based assessments.
   - Management of risk, including risk control, reduction of risk, avoidance of risk, assumption of risk, active defense, and transfer of risk (chain of trust agreements, insurance underwriting, warranties).
   - Disaster planning.
   - Psychosocial aspects of cybersecurity.
   - Ability to make and implement tough decisions.

3. **Law, Ethics, and Standards**
   - Federal, state, and local laws.
   - Applicable statutes.
   - International law.

- Legal implications of security measures and breaches.
- Ethical aspects of cybersecurity.
- Preemptive and proactive measures.
- Case studies of historical and current exploits.
- Standards and international organizations.
- Legal and regulatory aspects, including understanding of the judicial system, investigative processes, evidence chain, and incident reporting. What should be reported, and to whom?
- Incident response. What should students do if they know their computers are being hacked? (For example, should they report to the police, the FBI, or the campus CIO?)
- Preserving "after incident" potential evidence. Knowing how not to obscure or delete information.
- Testimony issues, such as expert witnesses.
- Forensics guidelines and protocols.

4. General Knowledge and Skills

- Accounting.
- Written and oral communications.
- Telecommunications.
- Strong technological foundation along with a desire to know how things work.
- Secretary's Commission on Achieving Necessary Skills (SCANS):
  - Planning and allocating resources.
  - Working with others as part of a team.
  - Acquiring and using information.
  - Understanding complex interrelationships.
  - Working with a variety of technologies.
- Customer relations.
- Internet use.
- Business knowledge.
- Strong verbal and writing skills, including levels of techno-speech.
- Management ability.
- Good judgment and common sense.
- Ethics.
- Discipline.
- Strategic and tactical thinking.
- Sense of humor. Not an actual requirement, but recommended. Without a sense of humor, students can burn out quickly.
- Creativity.
- Passion for job.

5. **Internet and Cybersecurity Skills and Knowledge**

A. **Software, Hardware, and Operating Systems**
- Strong technical knowledge of hardware and software.
- Operating systems (need to know more than one).
- UNIX.
- Default storage for password files.
- Cryptography.
- Programming.
- Application knowledge.
- Cross training.

B. **Network Security**
- Networks in telecommunications network security; for example, knowledge of networks, servers, systems, databases, signaling networks and gateways, network and element management systems, and network elements.
- Basic network security, information security, database security, system security, communications security, etc.

C. **Security Protocols**
- Confidentiality, integrity, availability, authentication, authorization, nonrepudiation, and privacy.
- Basic security standards for software development.
- Strong authentication and secure credentials exchange.
- Development and ensurance of compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Installation of centralized antivirus software.
- Fluency with firewalls and firewall installation.
- Antivirus, anti-Trojan horse, scanning, and backup.
- Upgrading of systems to software that is less vulnerable to attack.
- Smart cards and passwords.
- Biometrics.

D. **Threat Management**
- Styles of attack.

> "No one can argue today that there is any safety in the tangible world if in fact you don't have safety in the cyber world. There is now an intimate coupling and dependency between these things, and we are going to have to think of them in a more holistic way. . . . It is not about the narrow question of privacy versus security; it is the broader question of what do we all have to do as an industry in order to get computers to be a comfortably accepted infrastructure.
>
> —Craig Mundie, Senior Vice President and Chief Technical Officer, Advanced Strategies and Policy, Microsoft Corporation

- Psychosocial aspects of security.
- Identifying threats.
- Access and environmental management requirements.
- Policy and procedures security development.
- Knowledge of historical exploits.
- Possible future directions:
  - Verbal interfaces.
  - Brainwave analysis.
  - Nanotechnology.
  - Embedded devices.

6. **Knowledge of Industry Hiring Practices in Cybersecurity**
   Cybersecurity people are being trusted with the most important assets in the company. Companies generally
   - Run background checks to look for a history of malicious hacking or substance abuse and look at credit ratings. Companies want to make sure cybersecurity workers are not vulnerable to blackmail.
   - Place a high value on maturity, ethics, and integrity: "No hackers, crackers, or phreakers need apply."
   - Prefer cybersecurity workers who dress conservatively.
   - Want workers to know more than one operating system.
   - Do not hire people who have philosophical objections to big business, drug testing (many companies do not test, but applicants should not bring this up in an interview), the government, or college degrees and certifications.
   - Use college degrees and certificates not only to provide a measure of what people know, but also as an indication that workers can follow through and finish something that they start.
   - Want employees to have a combination of formal education and experience.
   - May use psychological profiling for certain positions.

Recommendations for Curricula, Courses, and Programs

1. Where possible, colleges should use modules that already exist and are available. These may be assembled into a coherent curriculum and adapted as needed.
2. A clearinghouse of existing resources should be assembled, possibly with the support of NSF.
3. Faculty need cybersecurity training to teach these new courses and programs.
4. Case studies of computer crimes should be incorporated into courses.
5. Better career counseling can help students chose the proper programs for their needs

and abilities. Counselors need computer and information technology training.

6. Two-year and four-year colleges must work together to achieve better articulation of programs and courses. When possible, this should occur at the faculty level.
7. Students who chose technician programs should be counseled about the job opportunities and career pathways open to them.
8. If students choose an associate of applied science program, they should be told that they will probably need additional mathematics and theory courses to enter a four-year computer or information management program, including mathematics courses such as discrete mathematics and calculus and computer courses such as data structures.
9. Community colleges should teach computer forensics and criminal justice to police reservists.
10. Students need to learn the fundamentals, then refine them in a hands-on, real-world, but controlled and safe environment. There must be continued study and practice after class sessions.

Aligning Programs between Two-Year and Four-Year Institutions

The workshop groups agreed that two-year and four-year institutions might not be able to align their cybersecurity programs easily, but that certain actions could help. The core curriculum at a two-year college can provide a foundation for more specific studies at the four-year level. Two- and four-year colleges need to coordinate and work jointly on problems and solutions. In some states, community college computer and IT courses and programs are designed to lead to employment, not to transfer. Some state systems exacerbate this problem.

Recommendations

To better align programs, community colleges and four-year colleges and universities could

1. Offer dual admission in two- and four-year programs, and cross-list courses.
2. Provide pathways by guaranteeing admission to a four-year college or university if a student completes a two-year program.
3. Inform students that if they take an associate degree program they will probably need to take additional courses, because the competencies taught at the technician level may not include the theoretical and analytical skills required by many computer and engineering B.S. programs.

4. Jointly develop programs to ensure that their programs are aligned. This requires constant dialogue between community colleges and four-year institutions.
5. Develop standards for model curriculum. For example, the Association for Computing Machinery (ACM) has developed programs that students can transfer from or take to prepare themselves for the workforce.
6. Keep transfer pathways open to students while recognizing that not all courses will transfer (for example, 45 credits might transfer rather than an entire degree of 60 or more credits).
7. Create bridge programs for students who need additional analytical and theoretical work.
8. Ensure that students have the option to be in programs whose primary purpose is to transfer (usually associate degree programs).
9. Provide transfer options from A.S. and A.A.S. programs to B.S. programs in business and management. A graduate of such a program might become a supervisor of technicians.
10. Teach core skills in the community colleges, including communication skills.
11. Develop articulation agreements that are regionally dependent.
12. Develop individual articulation agreements and understandings where needed.
13. Understand that no single program can teach all there is to know about law, ethics, or technology and that the depth of study and content must increase as the student advances.
14. Provide technical courses that will transfer, such as computer architecture, introduction to network communications, end user security (physical security and awareness), computer security (viruses, etc.), and network security (firewalls, Web security, etc.).
15. Discuss and plan with accrediting agencies the proper credentials of faculty teaching in workforce programs that will allow these programs to articulate with four-year institutions. Proper credentials might be a combination of work and academic experiences.
16. Ensure that all courses accepted for transfer are not just counted as core or electives, but that some are part of the four-year technical degree.

4. Preparation for Cybersecurity Positions

Many existing jobs in cybersecurity can be filled with people with two-year degrees. For example, a person with a two-year degree can be a network or security administrator or technician, and can use and deploy security systems. Two-year degrees can serve as the prerequisite for many industry-endorsed certifications. Students with four-year liberal arts degrees are good candidates for two-year college programs that combine technical courses with certification. Two-year programs can serve as the first two years of a bachelor's degree program. Workers with two-year degrees can be transitioned into security-related positions with additional education, experience, and preparation. The best academic preparation for many cybersecurity positions may be two associate degrees, one in network administration and one (or a certificate) in cybersecurity. Internships can be used to provide desired work experiences for entry into the workplace. Community colleges can provide both a strong academic program and hands-on activities. Nevertheless, while many entry-level positions can be met by students with two-year degrees, career advancement may require a bachelor's degree and work experience. For example, engineering, design, and integration positions require four-year degrees.

Current degree programs may not effectively provide the competencies required for higher-level positions in security. Cybersecurity workers may need specific cybersecurity training, but this training will be based on the premise that people possess fundamental knowledge and skills. Community colleges may provide students with an alternative to some of the major nonprofit or commercial providers of security training.

The examples of cybersecurity positions given below are not meant to be exhaustive, but are given to provide a range of positions and the corresponding academic preparation, work experiences, and certifications needed to fill those positions. Workshop participants emphasized that the education, experiences, and certifications needed are highly dependent on the requirements of a specific position and what tasks it involves. They commented that job titles may not tell the whole story.

Issues

1. For what cybersecurity occupations can industry-endorsed certification programs provide appropriate preparation?
2. For what cybersecurity occupations can two-year degree programs provide appropriate preparation?
3. For what cybersecurity occupations is a bachelor's degree or higher level of preparation needed?
4. What are the relative merits of degrees and certifications vs. work experience?

Cybersecurity Positions and the Academic Preparation, Work Experiences, and Certifications Needed to Fill Them

1. **Associate Degree Programs**
   - Tier 1 or entry-level person for customer service operations and help desk operations. The person who fills this position answers the phone and filters questions. These people can move into higher levels with additional experience and education.
   - Entry-level security administrator.
   - Network administrator.
   - Systems administrator.
   - Systems operator.
   - Paraprofessional IT occupations including graphics designers, Web developers, and digital content designers.
   - Tier 1 security telecommunications technician who performs tasks related to as surveillance, such as tracing calls and issuing subpoenas.

2. **Associate Degree Programs Plus Certifications or Work Experience**
   - Disaster recovery planning professional. DRI certification plus two years of education that includes five specific classes that can be added to other degrees or provided as special tracks.
   - System security professional. CISSP certification plus two years of education and experience.
   - Associate computer fraud examiner. CFE certification plus two years of education.
   - Advanced network administrator. Two or more years of experience plus two or more years of education.

- U.S. Department of Defense 2210 job series. Includes policy and planning, security, applications, operating systems, network services, data management, Internet, systems administration, and customer support.[1]

3. **Four-Year or Higher Degrees**
   - Certified information system auditor (CISA). CISA certification plus four years of education and two years of experience.
   - Computer fraud examiner. CFE certification plus four years of education
   - Designer.
   - Systems integrator.
   - Systems architect and developer.
   - Application developer.
   - Computer crime investigator.
   - Security systems engineer.[2]

4. **Four-Year or Higher Degrees Plus Certifications and Work Experience**
   - Policy advisor.
   - Business manager.
   - Designer of integrated network security and database management systems.
   - Risk management and vulnerability assessor. A four-year degree and 10 or more years of experience.
   - Corporate security provider. Highly dependent on position, but may require as much as 12 years of experience plus certifications.

> "We've seen that a number of major corporations have identified [cyber] security as their number one priority. When it comes to features versus security—security comes first. The same fundamental premise has to work in government. We have to have the words coming from the top and permeating to the rest of the government agencies that security is a [national] priority.
>
> —Howard A. Schmidt,
> Vice Chair,
> President's Critical Infrastructure
> Protection Board

Recommendations

1. Colleges and universities developing cybersecurity programs should examine the National Security Agency categorization of five security positions where skills are matched to different job descriptions.

[1] Even though there are no degree requirements for the 2210 series, many people who hold these positions have four-year degrees.

[2] Some workshop participants thought that two-year college graduates, particularly those with work experience, could serve as a security systems engineer. There was no consensus about this position, but more participants felt that a four-year degree was needed.

2. Two-year colleges, four-year colleges, and universities can make their programs more attractive to both prospective students and employers by
   - Working with employers to develop programs.
   - Establishing relationships with state, local, and federal governments.
   - Providing students with opportunities for meaningful research and work experiences.
   - Establishing local IT and security-related professional association chapters for students (for example, ACM).
   - Establishing IT and security-related community services.

3. Students can complement their academic experiences and build their portfolios by
   - Engaging in research.
   - Presenting research and other activities at professional society and trade association meetings.
   - Joining IT and cybersecurity organizations.
   - Participating in IT and cybersecurity community services.
   - Serving internships in IT or cybersecurity.
   - Engaging in IT or cybersecurity work opportunities.
   - Making sure that professors know them.

4. Government organizations should consider
   - Documenting requirements for cybersecurity positions.
   - Streamlining hiring processes.
   - Providing higher salaries for IT and cybersecurity professionals because many of these salaries are currently unrealistically low.

5. Advancing the Role of Community Colleges in Cybersecurity Education: Recommendations to Stakeholders

Workshop participants met in five breakout groups to make recommendations to support the role of community colleges in cybersecurity education. Each group made recommendations to the following stakeholder groups: community colleges; four-year colleges and universities; business and industry; professional societies and trade associations; and local, state, and federal government. Each breakout group included representatives from all the stakeholder groups. Results from these breakout groups are summarized below. These recommendations may, in some cases, duplicate recommendations made in other sections of this report.

What Community Colleges and Four-Year Colleges and Universities Should Do Together

1. **Form partnerships with each other and with business, industry, government, professional societies, and secondary schools to**
   - Share resources such as personnel, equipment, and curricula.
   - Develop faculty exchange programs.
   - Tap resources of vendors, IT user communities, and government agencies.
   - Identify the next generation of jobs.

2. **Undertake the coordination of educational programs by**
   - Developing transition programs ("2 + 2" or "2 + 2 + 2").
   - Sharing courses and cross-registering students.
   - Tracking students as they move through programs at different institutions.
   - Identifying career paths for students.
   - Designing complementary curricula to exploit the strengths of different types of institutions.

3. **Ensure student success by**
   - Monitoring students' progress in programs and providing counseling to retain students.

- Providing information to high school counselors so they can inform students about computing and security programs.
- Creating student-to-student mentoring programs.

4. **Market programs to the community by**
   - Educating presidents and CIOs of companies about the value of two-year and four-year programs.
   - Distributing advertisements and brochures about cybersecurity programs and educational pathways.
   - Preparing white papers for politicians at the local, state, and regional levels to inform them of the need for funding for cybersecurity programs.

5. **Provide services to the community, such as**
   - Hosting a cybersecurity conference for regional businesses, government agencies, and professional societies.
   - Working with businesses to offer cybersecurity training programs for existing employees.
   - Developing cybersecurity courses for local and state government personnel.
   - Hosting speakers on cybersecurity issues in conjunction with Infragard or other professional associations.

What Community Colleges Should Do

1. **Form partnerships to**
   - Define what cybersecurity technicians are and what jobs they can do in the workplace.
   - Develop modules, courses, and curricula for cybersecurity with other community colleges.
   - Educate all faculty and administrators about how cybersecurity modules, courses and curricula fit into the college curriculum.

2. **Ensure student success by**
   - Identifying career paths for students and current workers in cybersecurity and developing relevant materials and courses for groups that the community colleges serve (for example, students entering from high schools, people in the workplace desiring to upgrade skills or develop new skills, people changing careers, and students planning to articulate to a four-year institution).
   - Developing internships with business, industry, and government.
   - Providing scholarships.

- Showing that community colleges provide a way to transition between positions and educational levels.

3. **Find resources for programs by**
   - Conducting a market and needs analysis through queries or inventories of local businesses and government entities.
   - Approaching business and industry to form partnerships, secure advisors, and arrange internships for students and faculty.
   - Applying to grant programs.
   - Educating high-level administrators and trustees about cybersecurity programs and issues, and having them recognize that total costs may be above the average for other programs.

4. **Market programs by**
   - Demonstrating that a two-year degree is enough for a professional career.
   - Showing that community colleges can provide continuing education that allows current cybersecurity workers to maintain and improve skills.
   - Cultivating press attention.
   - Targeting special constituencies related to local needs and industries.

5. **Develop a broad-based approach to cybersecurity in the curriculum by**
   - Integrating cybersecurity concepts and topics into other computer and information courses and programs, as well as into business, law, economics, health care, and other courses and curricula.

6. **Ensure that faculty are well prepared by**
   - Developing cybersecurity externships for faculty in business, industry, and government.
   - Creating faculty exchange programs in which community college instructors teach university classes and vice versa.
   - Providing funds for faculty to enhance their cybersecurity skills by taking courses or attaining certifications.
   - Supporting faculty to attend conferences and workshops related to cybersecurity.
   - Providing differential pay for adjunct faculty with cybersecurity expertise.

What Four-Year Colleges and Universities Should Do

1. **Facilitate the articulation of programs and courses by**
   - Considering "reverse transfer" agreements, which allow students at four-year colleges and universities to take courses in community colleges that give them applied skills.
   - Fostering recognition of community college work in cybersecurity fields.
   - Building a fast track for program articulation with community colleges.
   - Developing complementary, not competitive, curricula.

2. **Ensure student success by**
   - Providing scholarship programs for transfers from community colleges.
   - Encouraging upper-level undergraduate and graduate students to mentor high school and community college students.

3. **Foster partnerships by**
   - Working with two-year colleges on joint projects, such as grants and centers.
   - Sharing classroom space or equipment and laboratories, either physically or through remote access.
   - Coordinating course schedules with community colleges.

4. **Ensure faculty expertise by**
   - Creating faculty exchanges and other joint professional development opportunities.
   - Offering more graduate courses that target community college faculty and fit their schedules.
   - Partnering with community colleges to have joint access to qualified instructors.

What Business and Industry Should Do

1. **Encourage workers to share their expertise by**
   - Serving as adjunct professors or guest lecturers.
   - Team-teaching with community college faculty.
   - Serving on advisory boards.
   - Acting as workshop leaders for professional development initiatives at community colleges.
   - Helping in the development of courses and programs.
   - Providing connections to industry leaders so that people preparing programs and doing fieldwork can be exposed to the needs of industry.

2. **Promote student success by**
   - Offering internships, particularly paid internships, for students.
   - Sponsoring scholarships, perhaps including a presidential scholarship in cybersecurity, to raise the awareness of cybersecurity programs in community colleges.
   - Supporting tuition reimbursement for current workers to study cybersecurity.
   - Providing job-shadowing opportunities for students in high schools, community colleges, and four-year colleges and universities.
   - Providing mentors to students to help them learn the good habits of mature professionals in the workplace.

3. **Ensure community college faculty expertise by**
   - Organizing workshops for faculty.
   - Inviting faculty members to use unfilled slots in industry or vendor training sessions.
   - Providing externships for faculty.
   - Sponsoring faculty memberships in professional associations.
   - Funding faculty positions (not necessarily chairs) at colleges and universities.

4. **Work in partnership with community colleges to**
   - Raise awareness of cybersecurity issues with college and university administrators.
   - Market programs to workers within companies and to the broader community.
   - Identify the needs and special areas that community colleges serve best.
   - Sponsor programs in association with community colleges, such as by underwriting a program or a lab.
   - Cross-list some industry training with community college offerings.
   - Use community college facilities and faculty to conduct workshops on cybersecurity.
   - Use students in current programs to give introductory cybersecurity workshops for business and industry.

What Professional and Trade Associations Should Do

1. **Work in partnership with business and industry to**
   - Identify leaders who will spur business and industry involvement with community college programs.
   - Market and advertise programs.
   - Expand current activities with four-year colleges and universities to community colleges.
   - Raise community college and university administrators' awareness of cybersecurity.
   - Release salary surveys of cybersecurity professionals.

2. **Ensure student success by**
   - Forming student chapters of professional organizations.
   - Providing students with scholarships and memberships in professional and trade associations.
   - Sponsoring student recognition awards and encouraging students to actively participate in meetings of professional and trade associations.
   - Promoting lifelong learning within career paths.

3. **Ensure faculty expertise by**
   - Sponsoring local and regional workshops.
   - Providing faculty memberships in professional and trade associations.
   - Supporting subscription services and online access to association publications.

What Local, State, and Federal Government Entities, including NSF, Should Do

1. **Support program development and implementation by**
   - Providing funding opportunities and holding institutions accountable for the use of funds.
   - Developing a program of workshops and courses to prepare cybersecurity faculty.
   - Finding ways to fast-track approval for programs and curricula.
   - Communicating and disseminating information and best practices.
   - Providing forums for sharing information.
   - Supporting the development of a cybersecurity clearinghouse Web site that links community colleges that currently have or are developing cybersecurity programs and provides other resources, including educational materials, curricula, and information about faculty development opportunities. This might become part of the National Science Digital Library (NSDL) supported by NSF.
   - Hosting national and regional events with presidents and deans and stressing to them the national need for cybersecurity programs.
   - Supporting the recognition of community college programs.
   - Using community college resources to grow local government security programs.

2. **Work together to**
   - Share cybersecurity information and practices among levels of government.
   - Encourage government agencies to provide job descriptions and titles that are appropriate for community college cybersecurity graduates.
   - Develop awareness of cybersecurity across the educational spectrum.
   - Sponsor workshops to bring academia, industry, and government together.

- Review practices concerning government contractors and required degrees (in many places contractors are currently required to have a four-year degree to perform jobs that might be performed by associate degree holders).

3. **Ensure faculty expertise and student success by**
   - Supporting internships (if possible, paid ones) for students.
   - Supporting paid externships for faculty.
   - Supporting outreach to community colleges by the NSA Centers of Excellence.
   - Adding community college students to those served by NSA Centers of Excellence.
   - Providing information to community college programs so that graduates of both two- and four-year institutions know how to apply for government openings in cybersecurity.
   - Encouraging the use of current educational programs supported by the Department of Defense and Department of Energy as a source of educational materials, curricula, and adjunct professors.

4. **Work with community colleges directly by**
   - Providing members for advisory committees.
   - Offering guest speakers.
   - Encouraging cybersecurity experts to teach as adjunct faculty.
   - Providing expertise in curriculum development.
   - Sponsoring field trips for students to agencies with cybersecurity interests.
   - Marketing and publicizing programs.
   - Communicating success stories.

> **Doing a better job of what we have been doing is not the solution to the computer security problem. It is the only thing we can do right now, but ultimately we need long-term basic research. We need to build a cadre of researchers who think deeply about these problems and think about them in a different way.**
>
> —William A. Wulf,
> President,
> National Academy of Engineering,
> and AT&T Professor of
> Engineering and Applied Science,
> University of Virginia

White Paper

6. Case Study: Creation of a Degree Program in Computer Security

Barbara Belon, Norwalk Community College
Marie Wright, Western Connecticut State University

Introduction

This paper describes the process of creating a degree program in computer security at Norwalk Community College (NCC) in partnership with a program option in information security management at Western Connecticut State University (WCSU). The events are described in chronological order, as follows:

The Awareness and Verification of Need: April 2001
The Research: April 2001–May 2001
The Idea: June 2001
The Contacts: July 2001–October 2001
The Process: October 2001–January 2002
The Degree Approval Process: February 2002–September 2002

Awareness and Verification of Need

In April 2001, a number of articles about the scarcity of trained computer security professionals in the United States appeared in national information technology (IT) periodicals, including *ComputerWorld, eWeek, Information Week,* and *InfoWorld*. These articles discussed a high demand for these individuals in both the public and private sectors, and the scarcity of applicants who are qualified for cybersecurity jobs. Upon reading some of these articles, Barbara Belon, director of the Center for Information Technology at Norwalk Community College, Connecticut, decided to verify that there was indeed such a shortage of trained computer security professionals among companies in the Norwalk region.

Fairfield County, where the college is located, is heavily populated with companies that create IT products and provide IT services. Belon informally contacted

the chief information officers (CIOs) of several of these companies. All of them confirmed that they had serious problems hiring qualified computer security personnel. In particular, Patricia Fisher, CEO of Janus Associates, said that finding qualified candidates was difficult and that she was continually on the lookout for prospective computer security employees. Barry Monies, CEO of Computronix and Computronix Computer Systems, echoed those sentiments. Although these companies were busy and growing, they were finding it difficult to find entry-level job seekers who had any preparation in computer or information security. CIOs who belonged to the local Society for Information Management (SIM) chapter said that their companies either were searching for qualified computer security professionals or had given up the search because their job postings had not yielded any viable candidates.

This informal survey made it clear that there was a mismatch between those who needed skilled professionals and those who could provide qualified candidates.

The Research

In late April 2001, research began in earnest to search for existing computer and information security education programs. Belon, assisted by a team of researchers, used several Internet search engines (including Google, Lycos, and AltaVista) to locate colleges and universities with accredited degree programs in either computer security or information security. They found many master's and doctoral degree programs in computer science and information systems. In most of these programs, information security or cryptography were elective, not required, courses. Twenty-three institutions were certified as NSA Centers of Academic Excellence in Information Assurance Education. The researchers found no degree programs in cybersecurity at the bachelor's level, and only one at the associate's degree level, at Texas State Technical College in Waco, Texas. That 71-credit hour program leads to an associate of applied science in network security technology degree. It focuses on computer networks and operating systems, and includes security assessment and e-commerce security courses that prepare students for careers on corporate security teams.

The researchers found that almost all programs for training computer security and information security professionals were at the master's and doctoral degree levels. It was no wonder that there were not enough entry-level security professionals to meet corporate demand. The single Texas State Technical College program alone could not produce the numbers needed for the U.S. market.

The researchers determined that the country needed more undergraduate degree programs that were focused on computer and information security in order to satisfy the growing demand for professionals in this relatively new field.

The Idea

In June 2001, Belon presented the idea of developing a new degree program in computer security to NCC's president and academic dean. They both endorsed the idea and urged Belon to continue with her research and to make contacts at universities with graduate programs in computer security or information security. The president put degree program development on the agenda for the next meeting of the president's IT advisory committee, which is composed of CIOs and CEOs from area companies. At their June meeting, the committee members approved the idea of developing a computer security degree at NCC, articulated with a four-year school.

The Contacts

K. C. Senie, who is NCC's director of grants and strategic planning, helped Belon identify personnel in university computer security programs. One of her contacts was Alan Berg, administrative director of the INFOSEC program at James Madison University (JMU) in Harrisonburg, Virginia. While discussing JMU's program and NCC's desire to partner with a four-year institution, Berg suggested that Senie contact Marie Wright, a faculty member at nearby Western Connecticut State University.

Near the end of August 2001, Senie contacted Wright and they began discussing the possibility of jointly developing a degree program in computer security. They proposed that NCC offer introductory security courses and hands-on lab courses in networks and operating systems while WCSU offer more advanced theoretical courses in information security through its existing information security management program.

On September 14, 2001, faculty and administrative representatives from NCC, WCSU, and Connecticut Technology College met to dicuss NCC's proposal to develop an associate degree program in computer security that would mesh with WCSU's existing bachelor's degree program in management information systems (MIS)/information security management (ISM). They also discussed developing program articulation between NCC and WCSU and the potential for creating articulations with other four-year institutions in the state.

After the meeting, Belon prepared a draft articulation agreement that paired the general college core courses in WCSU's degree requirements with those offered at NCC. The agreement was delivered to WCSU on September 26, 2001, and approved by WCSU's MIS department and administration shortly thereafter.

During the last week in September, Belon and Wright began to assemble an advisory committee of computer and information security professionals from the region for the purpose of creating the new degree program. At Belon's request, the local Society for Information Management chapter in Fairfield County e-mailed its members to tell them about NCC's

proposed computer security program and to ask those with relevant work experience to contact Belon if they were interested in helping to draft the program and course content. The e-mail was sent on October 2, 2001. On October 3, Belon got calls from 12 security professionals from government, academia, and industry who were all interested in participating in the degree development process.

The new Computer Security Advisory Committee was at first composed of 16 persons. Five committee members became unable to participate, and so the committee ultimately consisted of 11 members. Two of these were from NCC. Four were actively involved in the security endeavors of four area businesses: Allied Domecq PLC, Janus Associates, Swiss Reinsurance, and Unilever. Two committee members were from the Connecticut State Police and one was from the Norwalk Police Department. Two were from four-year higher education institutions in the region, Sacred Heart University and WCSU.

The Process

The first Computer Security Advisory Committee meeting took place on October 24, 2001. At this meeting, the members were charged with developing three items:

1. A list detailing the *knowledge and skills* needed by entry-level computer security professionals.
2. A list of the knowledge and skill *components* that could be taught in a formal program of study, as opposed to the ones that are learned on the job.
3. A document that grouped the knowledge and skill components identified into logical course delivery units that identified components that were not covered by existing courses at NCC or WCSU (that is, a "gap analysis").

In the next two months, the following was accomplished:

Knowledge and Skills List

Most of the October 24 meeting was spent on developing the knowledge and skills list. The committee members first listed the skills needed for jobs in computer and information security. Then they discussed the items, adding more skills, deleting others, and combining some skills to make the list clearer. The committee also began defining entry-level security positions and what skills they might require.

On October 30, 2001, Belon and Wright met at WCSU to recap the first advisory committee meeting and to move the knowledge and skills list to the next level. First, they used numerous security job descriptions that Wright had compiled from online regional job postings to supplement the list. They then incorporated into the list the knowledge and skills identified by two certification bodies, such as SANS (the System Administration, Networking and

Security Institute)[1] and (ISC)[2], the International Information Systems Security Certification Consortium, Inc.[2] Their objective was to synthesize the knowledge and skill requirements before the next advisory committee meeting so that the committee members could then review and modify the list.

Belon and Wright e-mailed their finished list to the committee members, directing them to review the items and be prepared to support their inclusion, deletion, or modification at the next advisory committee meeting.

Components

The second Computer Security Advisory Committee meeting was held at NCC on November 14, 2001. The committee decided that, rather than concentrate on the specific knowledge and skills required for particular security jobs (such as security analyst or security administrator), they would put job titles aside in order to produce a list of the critical knowledge and skill components that the students should have in order to pursue productive careers in computer and information security. The list was added to and revised during the course of the meeting.

On November 27, Belon and Wright met at WCSU. Wright had reorganized the knowledge and skill requirements identified by the committee into categories that aligned with the (ICS)[2] Common Body of Knowledge topical areas. She has also supplemented the knowledge and skills list with additional requirements from (ICS)[2] and the National Security Telecommunications and Information Systems Security (NSTISS)[3] standards.

The committee met for the third time on November 28 again at NCC. The committee sequenced and finalized the knowledge and skills list and reached final agreement on the content of the computer security degree program.

The committee agreed that Belon and Wright would match the identified knowledge and skills to the content of current courses at NCC and WCSU.

---

[1] SANS offers several Global Incident Assurance Certifications. Beginners' certifications include the GIAC Security Essentials Certificate (GSEC), the GIAC Security Leadership Certificate (GSLC), the GIAC Information Security Officer-Basic Certificate (GISO-Basic), and the GIAC IT Security and Audit Kickstart Certificate (GIAK). Information on these and other GIAC certificate offerings can be found at www.giac.org

[2] (ICS)[2] has identified a common body of knowledge (CBK) necessary for certification as a certified information systems security professional (CISSP). The CBK is embodied within 10 domains: security management practices; access control systems; telecommunications and network security; cryptography; security architecture and models; operations security; applications and systems development; business continuity planning and disaster recovery planning; law, investigation, and ethics; and physical security. Information about the (ICS)[2] and CISSP credential can be found at www.isc2.org.

[3] To be accredited by the National Security Agency as a Center of Academic Excellence in Information Assurance Education, an educational institution must show that it meets certain criteria, among them that the academic program maps to five NSTISSI standards: NSTISSI 4011 (National Training Standard for Information Systems Security Professionals), NSTISSI 4012 (National Training Standard for Designated Approving Authority), NSTISSI 4013 (National Training Standard for System Administration in Information Systems Security), NSTISSI 4014 (National Training Standard for Information Systems Security Officers), and NSTISSI 4015 (National Training Standard for Systems Certifiers). Details on these NSTISSI standards are located at www.nstissc.gov/html/library.html.

Courses and Gaps

In December 2001 and through January 13, 2002, Belon and Wright worked to identify existing NCC and WCSU courses that covered the knowledge and skill requirements the committee had identified. Any program skills and knowledge components that could not be matched with existing course content were referred to as gaps. After identifying these, Belon and Wright determined how they might be provided by new courses. Belon initially outlined four new courses to fill the gaps, but after further analysis, she and Wright agreed that the number of new courses required could be reduced to three.

During this time frame, Belon also wrote the degree application package that would be submitted to the Connecticut approval bodies who would accredit and license the program.

On January 16, 2002, the Computer Security Advisory Committee met at NCC. The committee members reviewed the course coverage and sequencing that Belon and Wright had prepared, examined the content of the three proposed courses, and made suggestions about the course sequencing. They raised minor questions about where data encryption would fit into the curriculum, whether there was enough coverage of the nontechnical aspects of information security (such as social engineering and the disposal of sensitive media), and whether the quantitative aspects of information security (such as financial planning and cost-benefit analyses) would be covered. They were able to get the answers to these questions by reviewing the content that Belon and Wright had proposed for selected courses. The members present gave their approval for moving the completed degree application forward through the academic approval process. During the following week, the committee members who had not attended the January 16 meeting e-mailed their approval.

Appendix 1 shows the final list of knowledge and skill requirements that the committee identified and the NCC and WCSU courses that covered those requirements. Appendix 2 provides course descriptions.

By the end of January 2002, the committee had revised the program articulation agreement between NCC and WCSU to streamline the student transfer process.

The Degree Approval Process

The formal application for accreditation and licensure of the associate of science in computer security was presented to the NCC Computer/Information Systems department at its February, 2002, meeting. The department approved the three proposed security courses and the total degree package. Immediately afterwards, the application received the academic dean's support and signature. The degree package then was forwarded to the NCC Curriculum Committee chairperson for distribution and action at that committee's March 20, 2002, meeting.

At the early March meeting of the president's IT advisory committee, the president of NCC was urged to call a special faculty meeting in order to expedite faculty approval of the computer security degree program. He acted accordingly and scheduled the meeting for April 8, 2002.

At its meeting, the NCC curriculum committee voted to approve the computer security degree program and the three new courses. However, at the end of the meeting, concerns were raised that the liberal arts requirement might not be met, depending on the electives a student selected. Since there was a chance that the degree program would be voted down when it was presented to the full faculty on April 8, Belon successfully petitioned the curriculum committee to accept a one-course addition of another liberal arts elective to the application.

On April 8, 2002, the NCC full faculty met and approved the degree application. The meeting was contentious. Although the substance of the degree program received strong faculty support, a major concern was expressed over the novelty of a two-year computer science program articulating with a four-year MIS degree program in a business school. Such a concern indicates how unusual a collaboration between computer science and a technical business discipline really is, and why the NCC/WCSU partnership is particularly noteworthy.

The full degree program package was sent to the Connecticut Community College Board of Governors on April 10, 2002. Over the next three weeks, the board's central office staff reviewed the application and called for minor changes. The application was then sent out for review. The Board of Governors unanimously approved the computer security degree program at its June 17 meeting. The final step will require the application package to be presented to the Connecticut Board of Higher Education for accreditation and licensure in September 2002.

Conclusion

Many more undergraduate degree programs are needed to meet the growing demand for cybersecurity professionals in the public and private sectors. In order to better address regional needs for security professionals, two-year and four-year educational institutions should involve area business and government professionals in the curriculum development process. The benefits of such a collaborative process are numerous: improved working relationships, new working relationships, additional networking opportunities, enhanced goodwill, and added public exposure for the organizations and educational institutions involved. In addition, stronger ties and high-quality programs articulated between two-year and four-year institutions provide lasting benefits to students and faculty as well as to regional businesses. Both NCC and WCSU believe that the process followed in developing the computer security degree program has produced a high-quality program that will greatly benefit our institutions and our regional constituents.

Appendix I:
Knowledge and Skill Requirements/Course Coverage

Knowledge of Access Control Systems

	Courses at WCSU	Courses at NCC
Identification, authentication, nonrepudiation	MIS 341/361	CMP 111
Account creation and termination (user access rights administration)		CMP 230
Biometric hardware/software used in conjunction with access control systems	MIS 341/389	CMP 251
Passwords (e.g., cracking/defensive cracking, guidelines for good passwords)	MIS 341/361	CMP 111
Access Control List/Access Control Matrix	MIS 341	CMP 230/117
File system permissions		CMP 230/251
Discretionary and mandatory access controls	MIS 341	CMP 230
Multilevel security (e.g., subject clearance levels)	MIS 341	
Audit logs	MIS 341/361	CMP 230/251

BEST COPY AVAILABLE

Knowledge of Telecommunications and Network Security

	Courses at WCSU	Courses at NCC
Media (e.g., twisted pair, coaxial cable, fiber optics, microwave, satellite)	MIS 260/341/385	CMP 107/117
LAN topologies (e.g., star, ring, bus)	MIS 260/341/385	CMP 117
Wireless technology	MIS 260/341/385	
LAN access methods (e.g., Carrier Sense Multiple Access/Collision Detection)	MIS 260/341/385	CMP 117
E-mail servers, routers, remote system access	MIS 385	
Protocols: (e.g., International Standards Organization Model of Architecture for Open Systems Interconnection, TCP/IP, Secure Sockets Layer, Secure Electronic Transaction)	MIS 260/341/385	CMP 111
Standards (e.g., IEEE 802.11)	MIS 341/385	CMP 117
Telephony and Private Branch Exchange (PBX) security	MIS 385	
Threats: (e.g., eavesdropping/wiretapping, traffic analysis, replay attacks, electromagnetic radiation interception, scanners, sniffers, Domain Name Server attacks, IP spoofing, Denial of Service/ Distributed Denial of Service attacks—message flooding, buffer overflow attacks)	MIS 341/361/385	CMP 111/253
Controls: (e.g., encryption, traffic padding, digital signatures, firewalls, intrusion detection systems, penetration testing, vulnerability scanning, Virtual Private Networks)	MIS 341/361	CMP 111/253

BEST COPY AVAILABLE

Knowledge of Cryptography

	Courses at WCSU	Courses at NCC
Terminology (e.g., plaintext, ciphertext, cryptanalysis, key, algorithm, block cipher, stream cipher)	MIS 341/361	CMP 111
Symmetric cipher systems (e.g., Data Encryption Standard, Advanced Encryption Standard)	MIS 341/361	CMP 111
Asymmetric cipher systems (e.g., RSA algorithm, Diffie-Hellman)	MIS 341/361	CMP 111
Escrowed encryption (e.g., Clipper Chip)	MIS 341	
E-mail encryption (e.g., Pretty Good Privacy)	MIS 341	CMP 111
Digital signatures	MIS 341/361	CMP 111
Digital certificates	MIS 341/361	CMP 111
Public Key Infrastructure (PKI)	MIS 361	CMP 111

Knowledge of Security Architecture

	Courses at WCSU	Courses at NCC
Memory (e.g., random access memory, read-only memory, cache, proxy cache)	MIS 260/341/389	
Evaluation criteria (e.g., Trusted Computer System Evaluation Criteria, Common Criteria)	MIS 341	
Confidentiality models (e.g., Bell-LaPadula)	MIS 341	
Integrity models (e.g., Biba)	MIS 341	
Availability	MIS 341/389	
Object classification levels	MIS 341	

BEST COPY AVAILABLE

Knowledge of Operations Security

	Courses at WCSU	Courses at NCC
Controls (prevent, detect, recover)	MIS 341/361	CMP 256
Separation of duties	MIS 341	CMP 256
Least privilege	MIS 341	CMP 256
Social engineering	MIS 341/361	CMP 256
Malicious code: Trojan horses, viruses (e.g., boot sector, program (file), macro), bombs (e.g., logic, time), trapdoors, worms, controls (e.g., prevention/inoculation, antivirus policy/software, backups)	MIS 341/361	CMP 111

Knowledge of Applications Security

	Courses at WCSU	Courses at NCC
Systems development life cycle	MIS 260/481	
Identify, document, and report security risks related to technical implementations		CMP 256
Configuration management	MIS 341	
Change management		
Database Security:		
Multilevel databases	MIS 301/341	
Threats to confidentiality (e.g., direct attack, inference exposures)	MIS 301/341	CMP 111
Threats to integrity (e.g., unauthorized additions/deletions/ modifications, propagation of errors)	MIS 301/341	CMP 111
Controls (e.g., suppression, concealing, privilege reduction, role-based access controls, partitioning)	MIS 301/341	

BEST COPY AVAILABLE

Knowledge of Legal and Ethical Issues

	Courses at WCSU	Courses at NCC
Privacy and security legislation (e.g., Freedom of Information Act, Family Educational Rights and Privacy Act, Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Health Insurance Portability and Accountability Act, Privacy Act)	MIS 341/361	CMP 111 (partial)
Intellectual property (e.g., patent, copyright, trade secret)	MIS 341	CMP 111
Investigation (e.g., gathering and handling evidence)		CMP 256
Global considerations (legal, ethical, cultural)	MIS 341/361	CMP 111
Encryption issues	MIS 341/361	

Knowledge of Security Management Practices

	Courses at WCSU	Courses at NCC
Security policies and procedures development (evaluate, develop, document, communicate, and implement)		CMP 256
Risk analysis/Risk assessment	MIS 341/361	CMP 111
Auditing (e.g., policies, guidelines, procedures)	MIS 361	
Security monitoring, testing, and evaluation		CMP 256
Security reviews and spot monitoring		CMP 256
Security maintenance		
Security education and awareness	MIS 341/361	CMP 256
Business Continuity/Emergency Response/Disaster Recovery Planning	MIS 341/361	

BEST COPY AVAILABLE

Other Knowledge

	Courses at WCSU	Courses at NCC
Physical security (e.g., fire suppression, guards, locks, alarms, disposal of sensitive media)	MIS 341	
Written, verbal, analytical, diagnostic, project management and problem-solving skills	MIS 341/361/ 481/495	ENG 101/102
Human relations skills		
Business processes; business metrics and reporting	MIS 481/495	
Desktop applications	MIS 260/405	CMP 101
Methods for keeping current in profession		
Understanding of security goals (confidentiality, integrity, availability, authentication, nonrepudiation)	MIS 341/361	CMP 111
Knowledge of system security tools and applications	MIS 361	CMP 111
NT administration (e.g., setting registry keys, setting up a safe file system, secure account policies, backups, auditing, monitoring and responding to incidents)		CMP 251
UNIX administration (e.g., securing workstation/server, packet firewalls, backups, auditing)		CMP 230/251

Legend:

WCSU Courses

MIS 260 Information System Concepts
MIS 341 Information Systems Security
MIS 361 Information Assurance
MIS 385 Fundamentals of Data Communication
MIS 389 Information Systems Hardware
MIS 405 Business Applications Using Microcomputers
MIS 481 Management Information Systems
MIS 495 Seminar in Management Information Systems

NCC Courses

ENG 101 Composition
ENG 102 Literature and Composition
CMP 101 Computer Concepts with Applications
CMP 107 Networking 1
CMP 111 Internet Commerce Technology
CMP 117 Networking 2
CMP 230 Operating Systems
CMP 251 Operations Security Technology
CMP 253 Network Security Technology
CMP 256 Security Management Practices

BEST COPY AVAILABLE

Appendix 2:
Course Descriptions

Norwalk Community College

Course No.	Course Title and Description
ENG 101	Composition (3 semester hours) This course develops students' ability to write effective essays and to reason critically. A review of grammar and syntax, as needed, is included. The goals of unity, coherence, and logical development are pursued through analysis of professional and student essays and through practice in prewriting, writing, and revision techniques. Students learn various organizational patterns. Students write and revise several essays.
ENG 102	Literature and Composition (3 semester hours) This composition course is a continuation of work in skills begun in ENG 101. Students receive further instruction in composition and write frequently in and out of class. The analytical and critical essays they produce focus on fiction, drama, and poetry. To prepare for these writing tasks, students learn how to read and appreciate various literary genres, how to interpret literature, and how to explain and support their ideas in writing. In addition, students complete a research paper on a literary topic.
CMP 101	Computer Concepts with Applications (4 semester hours) An introduction to computer concepts: input, output, processor, hardware, and software with emphasis on the information processing cycle, problem solving and algorithm development. A programming language is used to introduce students to programming and for developing solutions to common computing problems. Students also learn to use the computer as a tool by gaining experience with popular application software packages and the Internet. Three hours of class work, two hours of laboratory work.
CMP 107	Networking 1 (4 semester hours) An introduction to computer networking concepts. Topics include the functions of the ISO/OSI reference model; data link and network addresses; the function of a MAC address; data encapsulation; the different classes of IP addresses (and subnetting); the functions of the TCP/IP network-layer protocols. Student learn to plan, design, and install an Ethernet LAN using an extended or hierarchical star topology; to select, install, and test cable and determine wiring closet locations; and to perform beginning network maintenance, tuning, and troubleshooting along with basic documenting, auditing, and monitoring of LANs. This course consists of lecture- and computer-based training, as well as hands-on laboratories. Three hours of class work, two hours of laboratory.
CMP 111	Internet Commerce Technology (3 semester hours) This introductory course covers the current technologies supporting today's Internet commerce initiatives and the security issues surrounding conducting commerce on this Web platform. Some of the technologies explored in the course include digital certificates, payment systems, Web server tools, and security interventions.

BEST COPY AVAILABLE

Norwalk Community College (continued)

Course No.	Course Title and Description
CMP117	Networking 2 (4 semester hours) Instructional topics include safety, networking terminology and protocols, network standards, LANs, WANs, OSI models, Ethernet, Token Ring, Fiber Distributed Data Interface, TCP/IP addressing protocols, dynamic routing, and the network administrator's role and function. Particular emphasis is given to the use of decision-making and problem-solving techniques in solving networking problems.
CMP 230	Operating Systems (4 semester hours) Study of traditional operating systems, memory management systems, process scheduling and management methods, and file systems. Case studies on selected operating systems. Laboratory work in a closed classroom environment includes getting started with UNIX, UNIX shell interpreter, C and shell programming, pipes and filters, I/O systems, UNIX editors, file system structure, and network and system administration. Three hours of class work, two hours of laboratory.
CMP 251	Operations Security Technology (3 semester hours) Covers the identification of the controls over hardware and media, and the operators with access privileges to any of these resources. Addresses the resources that must be protected, the privileges that must be restricted, the control mechanisms available, the potential abuse of access, the appropriate controls, and the principles of good practice.
CMP 253	Network Security Technology (3 semester hours) Network security encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media. This course gives students the knowledge and hands-on practice in network security software, including preventive, detective, and corrective measures.
CMP 256	Security Management Practices (3 semester hours) Security management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability of those assets. This course prepares students to understand the planning, organization, and roles of individuals involved in security; develop security policies; and utilize management tools to identify threats, classify assets, and rate vulnerabilities.

BEST COPY AVAILABLE

Western Connecticut State University

Course No.	Course Title and Description
MIS 260	Information Systems Concepts (3 semester hours) This course provides students with the information systems fundamentals necessary to operate effectively in a computerized business environment. The course provides an overview of the components, operations, and roles of information systems in business environments. Major concepts and recent developments in computer hardware, software, telecommunications, and database management technologies are presented, and the strategic, global, and ethical dimensions of information systems are discussed.
MIS 341	Information Systems Security (3 semester hours) This course addresses both the behavioral and technological issues of information systems security. Topics include physical protection, hardware and software controls, encryption techniques, network and telecommunications security, malicious code, computer security legislation, contingency planning, and disaster recovery.
MIS 361	Information Assurance (3 semester hours) This course examines both offensive and defensive information security practices using scenarios and case studies. Topics include social engineering, corporate espionage, destruction and modification of data, control and disruption of information flow, electromagnetic signal interception, denial of service, cryptography, authentication methods, access controls, firewalls, intrusion detection systems, and risk assessment.
MIS 385	Fundamentals of Data Communications (3 semester hours) This course is intended for students who have a basic understanding of MIS and need to complement it with fundamental knowledge of data communications. The course focuses on understanding the alternatives in hardware, software, and transmission facilities; putting that understanding to work by making informed decisions; and integrating and implementing these decisions into a cohesive data communication system design.
MIS 389	Information Systems Hardware (3 semester hours) This course is intended to expose students to the hardware side of MIS. Hardware technology is currently several generations ahead of the software industry. As a result, a good foundation in hardware, as it relates to supplying current and future business solutions, is essential to the well-rounded MIS professional. Students will engage in hands-on activities related to hardware. The course discusses current hardware technology, its history, and its future; costs and planning for expansion; upgrading vs. replacing; total cost of ownership; and how to stay current with hardware.
MIS 405	Business Applications Using Microcomputers (3 semester hours) Presents commonly used microcomputer software packages as a tool for the business user. Packages learned will span the business disciplines, including marketing, finance, accounting, employee relations, and manufacturing.

BEST COPY AVAILABLE

Western Connecticut State University (continued)

Course No.	Course Title and Description
MIS 481	Management Information Systems (3 semester hours) An analysis of the impact of computer-based information systems on decision-making, planning, and control; the changes in organizational structures needed to accommodate information technology; and the design of information systems to facilitate management of the functional areas within a firm.
MIS 495	Seminar in Management Information Systems (3 semester hours) This is the capstone course for MIS majors. The course covers techniques for the use of computers in both decision making and information processing. The systems approach is used to integrate systems theory with practical experience.

BEST COPY AVAILABLE

White Paper

7. Cybersecurity Education in Community Colleges across America: A Survey of Present and Planned Implementation

Robert D. Campbell, Rock Valley College
Elizabeth K. Hawthorne, Union County College

Introduction

Since September 11, 2001, Americans have been more aware than before of potential threats to computer system security and of the urgent need to quickly and effectively educate and expand the cybersecurity workforce. Education in cybersecurity and information assurance falls into two distinct categories: training, which emphasizes particular systems, situations, and environments rather than broad principles; and scholarship, which emphasizes underlying principles, concepts, and their applications. These two categories must complement one another.

This paper describes a variety of existing and planned efforts for addressing cybersecurity education in community colleges across America. It discusses four ways that such instruction is packaged at two-year colleges and describes specific activities at several institutions in sufficient detail to provide insights into those efforts and to suggest the direction that might be taken by other community colleges that are interested in offering education in cybersecurity.

Four ways of packaging cybersecurity instruction are

- The Degree Program—A four-semester program of study leading to an associate degree. Intended to prepare students for immediate employment or for transfer into baccalaureate studies in the field of computing, with special emphasis on careers related to cybersecurity and its associated fields.
- The Certificate Program—A two-semester program of study leading to an institution-conferred certificate. Intended to provide an abbreviated program of study to augment the institution's degree programs and to give students the opportunity to obtain specialized training in cybersecurity.

BEST COPY AVAILABLE

- The Course—A credit course that is part of an existing program of study. Intended as an elective or a required component in a program of study that is not focused on cybersecurity, providing students with an introduction to these topics.
- The Credential Program—A noncredit program of preparation for an industry certification. Intended to specifically prepare students to sit for targeted industry certification exams in cybersecurity; not necessarily related to credit program offerings.

These four approaches to cybersecurity education are available to most comprehensive community colleges and are familiar to faculty and administrators in this sector of higher education. Some two-year colleges in the United States have already availed themselves of these avenues for addressing cybersecurity education. Other community colleges may be poised to do likewise, once model implementations are publicized and the skill sets for computer security instruction are better identified.

Degree Program Implementations

Current Implementations at Seminole Community College

An A.S. degree in the Florida community college system is typically a career education degree, not intended for transfer, equivalent to the associate of applied science (A.A.S.) degree in many other states. According to Seminole Community College (SCC) in Sanford, Florida, "A.S. programs provide [students] with the knowledge necessary to perform and excel in a particular profession. Some of the credits earned in an A.S. degree program can be transferred to a four-year college or university . . . however, the A.S. curriculum is not considered equal to the first two years of a bachelor's degree."

SCC offers an A.S. degree described as preparing graduates for career opportunities as Internet and network security specialists, Internet technical support specialists, Internet and network security technicians, and database security technicians. The program focuses on the security aspects of Internet commerce over multiple systems (Internet, intranet, and local systems), providing security skills for an e-business environment in the areas of security analysis; designing and creating a security system; troubleshooting security; testing security measures; and creating, implementing, and maintaining a security policy. It also addresses legal and ethical issues, current and emerging legislation, virus threats, accounts and groups, file systems, and network security.

This degree program consists of 63 semester-hour credits: 30 credits in major courses, 12 credits in support courses, 6 credits in electives, and 15 credits in general education, as detailed in Table 1 below.

Table 1. Credit Distribution for SCC's A.S. Degree

Course No.	Course Name	Credits
Major Courses		
APA 1111C *or* ACG 2021C	Office Systems Accounting I *or* Principles of Financial Accounting	3
CET 1652C	Computer Network Architecture	3
CGS 2069	Survey of e-Business Technology	3
CGS 2100C	Microcomputer Software Packages	3
COP 2066	Internet Web Essentials	3
GEB 1011 *or* GEB 1136	Introduction to Business *or* Foundations of e-Business	3
GEB 2442	e-Business Law and Ethics	3
MAN 2021 *or* MAN 2800	Introduction to Management *or* Small Business Management	3
MAN 2581	Project Management	3
MAR 2011	Marketing	3
	Subtotal:	**30**
Support Courses		
CEN 1543C	Introduction to Internetworking Security	3
CEN 2525	Advanced Internetworking Security	3
CET 2665C	Firewall Configuration and Management	3
CET 2760C	Web Server Management	3
	Subtotal:	**12**

BEST COPY AVAILABLE

Table 1. Credit Distribution for SCC's A.S. Degree (continued)

Course No.	Course Name	Credits
Electives (two from the three listed)		
CET 2662C	Security Testing and Auditing	3
CET 2664C	Encryption and Cryptography	3
CET 2666C	Configuring IP Security	3
	Subtotal:	**6**
General Education Courses		
ENC 1101	English I	3
SPC 1600	Introduction to Oral Communication	3
	Humanities General Education Elective	3
	Mathematics General Education Elective	3
	Social Science General Education Elective	3
	Subtotal:	**15**
	Degree Total:	**63**

Major Course Descriptions

- **APA 1111C—Office Systems Accounting I.** Focuses on fundamental financial record keeping and reporting using computers and general ledger software to automate record-keeping activities.
- **ACG 2021C—Principles of Financial Accounting.** Introduces students to preparing financial statements for partnerships and corporations.
- **CET 1652C—Computer Network Architecture.** Introduces the principles and methods behind local area networks and Internet/Web connectivity. (Prerequisite: CGS 2069—Survey of e-Business or CET 1486C—Network Concepts and Operating Systems.)
- **CGS 2069—Survey of e-Business Technology.** Focuses on communications, network concepts, Internet, World Wide Web, and e-Commerce fundamentals.
- **CGS 2100C—Microcomputer Software Packages.** Introduces students to major application software packages using Microsoft Office.
- **COP 2066—Internet Web Essentials.** Covers use of Web browsers to access Internet services; creation of simple Web pages; and concepts related to WWW, Internet, e-mail, Telnet, Gopher, security measures, and FTP. Nontechnical topics include legal, ethical, and privacy issues, and etiquette. (Prerequisites: CGS 2100C—Microcomputer Software Packages and CGS 2069—Survey of e-Business or CET 1486C—Network Concepts and Operating Systems.)

BEST COPY AVAILABLE

- **GEB 1011—Introduction to Business.** Provides an introduction and general overview of business.
- **GEB 1136—Foundations of e-Business.** Provides a functional and general view of e-Business and e-Commerce management strategies, and business-to-business (B2B), business-to-consumer (B2C), and intrabusiness models.
- **GEB 2442—e-Business Law and Ethics.** Provides an overview of Web-based business legal issues and aspects of intellectual property rights, including patents, copyrights, trademarks, and trade secrets.
- **MAN 2021—Introduction to Management.** Studies the essentials (planning, organizing, staffing, directing, controlling) of operational management in a business environment.
- **MAN 2800—Small Business Management.** Presents a fundamental approach to managing a small firm and the necessary steps in planning and evaluating small business concerns.
- **MAN 2581—Project Management.** Covers the concepts of project management for information technology using real-world examples.
- **MAR 2011—Marketing.** Introduces the marketing process: consumer behavior, product planning, marketing institutions and functions, and promotional and pricing strategies.

Support Course Descriptions

- **CEN 1543C—Introduction to Internetworking Security.** Examines the principles, mechanisms, and implementations of network security and data protection; company-wide security process and performing a security audit; controlling access to systems, resources, and data; and security issues of common operating systems. (Prerequisite: CET 1652C—Computer Network Architecture.)
- **CEN 2525—Advanced Internetworking Security.** Examines in greater depth the principles, mechanisms, and implementation of network security and data protection. (Prerequisite: CEN 1543C—Introduction to Internetworking Security.)
- **CET 2665C—Firewall Configuration and Management.** Examines how firewalls are used as a network security solution; network address translation; proxy servers inspection firewalls; basic VPNs; and intrusion detection systems. Emphasizes installing, configuring, and managing today's most popular software and hardware firewalls.
- **CET 2760C—Web Server Management.** Prepares students to set up, configure, and manage a complete Web server. Covers fundamental Web server security and other Web server–related issues. (Prerequisites: CET 1515C—Web Authoring, and CET 1492C—NetWare Administration.)

Elective Course Descriptions

- **CET 2662C—Security Testing and Auditing.** Focuses on establishing and using testing and auditing policies and installing, configuring, and using related software tools.
- **CET 2664C—Encryption and Cryptography.** Introduces basic theories and practices of cryptographic techniques for computer security; encryption (secret-key and public-key), digital signatures, secure authentication, e-Commerce (anonymous cash, micro pay-

ments), key management, cryptographic hashing, and Internet voting systems. (Prerequisite: CEN 1543C—Introduction to Internetworking Security.)
- **CET 2666C—Configuring IP Security.** Focuses on advanced IP security configurations, evaluating different protocols used to provide network services, identifying vulnerabilities in commonly used Internet service protocols, and concepts behind IP security protocol. (Prerequisite: CET 2665C—Firewall Configuration and Management.)

Planned Implementation at Tompkins Cortland Community College

Tompkins Cortland Community College in Dryden, New York, plans to implement a computer forensics degree program for the first time in the fall 2002 semester. The program will teach students how to provide a secure computer environment and how to collect and analyze computer-related evidence, and will prepare them for entry-level positions as data recovery technicians or members of security teams. Potential entry-level positions are identified as computer systems technician responsible for implementing procedures and software to maintain a secure computer environment for a business or other organization; computer technician helping law enforcement officials obtain evidence to be used in a court of law; and security staff member responsible for monitoring and supporting computer-based security systems.

Program requirements include a combination of criminal justice and computer technology courses. The program emphasizes social science and criminal justice coursework and developing intensive research skills. A dedicated lab provides hands-on experience with investigative tools and evidence gathering.

Core Courses

- Security System Design and Analysis (3 credits)
- Computer Forensics. Includes a lab component using industry software, such as Expert Witness (3 credits)
- Intrusion Detection. Includes a lab component using industry software, such as Smartwatch (3 credits)
- Search and Seizure—Legal and Privacy Issues (3 credits)
- Economic Crime Investigation (3 credits)
- Computer Forensics Coop/Fieldwork (6 credits)

Non-Core Courses

- Web Page Design (1 credit)
- Security System Design and Analysis (3 credits)
- Introduction to Computer Information Systems (3 credits)
- Network Design (3 credits)
- Operating Systems (2 credits)
- Administration of Criminal Justice (3 credits)

- Criminal Investigation (3 credits)
- Academic Writing I (4 credits)
- Fundamentals of Speech (3 credits)
- Liberal Arts Elective (3 credits)
- Statistics (3 credits)
- Introduction to Psychology (3 credits)
- Introduction to Sociology (3 credits)
- Introduction to Criminology (3 credits)
- Unrestricted Elective (3 credits)
- Wellness Requirement (2–3 credits)

Planned Implementation at Moraine Valley Community College

Many community colleges offer the Cisco Systems' Networking Academy program, which includes networking curriculum. Some also use sponsored curricula that accompany and extend the basic Cisco curriculum to address targeted topics and programs (see www.cisco.com/warp/public/779/edu/academy/overview/curriculum/). Currently under discussion is a new curriculum in the area of "security and data assurance" that may well become the next officially sponsored curriculum.

Moraine Valley Community College (MVCC) in Palos Hills, Illinois, is establishing an IT Security and Data Assurance Regional Academy in affiliation with the regional Cisco academy it operates under its designation as a Cisco Academy Training Center, and as a collaborative undertaking with the Cisco Learning Institute (www.ciscolearning.org/index.html). MVCC proposes to use this academy to undertake curriculum and program development, establish standardized assessment, provide training materials for instructors, and conduct professional development activities. The proposed curriculum includes six lower-division courses that would form the technical component for an A.A.S. degree in IT security and forensics. The proposed courses are

- Security Essentials
- Firewalls, Perimeter Protection, and VPNs
- Access Control Systems and Methodology
- Risk Assessment, Vulnerability, and Disaster Recovery
- System Forensics, Investigations, and Response
- Security Architecture, Models, and Case Studies

Planned Implementation at Norwalk Community College

Norwalk Community College in Norwalk, Connecticut, has plans currently awaiting approval by the Connecticut Board of Higher Education to offer an A.S. degree program in computer security that would articulate with a B.S. in management information systems/information security management degree at Western Connecticut State University. The degree requirements for the college's existing computer science program, which, along with

three new computer security courses are the basis of the proposed new degree program, can be reviewed at www.ncc.commnet.edu/programs/compscience.htm.

Certificate Program Implementations

A certificate program is an abbreviated program of study leading to an institution-conferred certificate. This type of study provides students with a computer networking background the opportunity to further develop specialized skills in cybersecurity.

Current Implementation at Seminole Community College

Seminole Community College in Florida offers an e-Business Security Technical Certificate that is a subset of the degree program described in the discussion above.

Current Implementation at Northern Virginia Community College

Northern Virginia Community College (NVCC) offers a career studies certificate in network security that is associated with the college's information systems technology efforts. The curriculum of this enhanced competency module prepares students for employment as network security specialists or Internet security specialists. The certificate program consists of 28 semester-hour credits, distributed as shown in Table 2.

Table 2. Credit Distribution for NVCC's Network Security Certificate

Course No.	Course Name	Credits
IST 245	Network Security Basics	3
IST 246	Network Attacks, Computer Crime, and Hacking	4
IST 247	Network Communication, Security, and Authentication	4
IST 248	Internet/Intranet Firewalls and e-Commerce Security	4
IST 266	Network Security Layers	4
IST 267	Legal Topics in Network Security	3
IST 293	Studies in Network Security	3
ENG/SPD	Elective	3
	Total:	28

BEST COPY AVAILABLE

Course Descriptions

- **IST 245—Network Security Basics.** Explores the basics of network security in depth, including security objectives, security architecture, security models, and security layers; the topics of risk management, network security policy, and security training; and the five security keys: confidentiality, integrity, availability, accountability, and auditability. (Prerequisite: an A.A.S. degree or higher in a networking field.)

- **IST 246—Network Attacks, Computer Crime, and Hacking.** Provides an in-depth exploration of various methods for attacking and defending a network; network security concepts from the point of view of hackers; attack methodologies, intrusion detection systems (IDS), malicious code, computer crime, and industrial espionage. (Prerequisite: an A.A.S. degree or higher in a networking field.)

- **IST 247—Network Communication, Security, and Authentication.** Provides an in-depth exploration of various communication protocols from the point of view of the hacker in order to highlight protocol weaknesses, with a concentration on TCP/IP; includes topics of Internet architecture, routing, addressing, topology, fragmentation, and protocol analysis; use of various utilities to explore TCP/IP. (Prerequisite: an A.A.S. degree or higher in a networking field.)

- **IST 248—Internet/Intranet Firewalls and e-Commerce Security.** Provides an in-depth exploration of firewall concepts, types, topology, and the firewall's relationship to the TCP/IP protocol; client/server architecture, the Web server, HTML, and HTTP in relation to Web security and e-commerce security; digital certification, X.509, and public key infrastructure (PKI). (Prerequisite: an A.A.S. degree or higher in a networking field.)

- **IST 266—Network Security Layers.** Provides in-depth exploration of the security layers needed to protect a network; physical security, personnel security, operating system security, software security, and database security. (Prerequisite: an A.A.S. degree or higher in a networking field and successful completion of the certificate program's first semester.)

- **IST 267—Legal Topics in Network Security.** Provides an in-depth exploration of the civil and common law issues that apply to network security; statutes, jurisdictional, and constitutional issues related to computer crime and privacy; rules of evidence, seizure, and evidence handling; court presentation; and computer privacy. (Prerequisite: an A.A.S degree or higher in a networking field and successful completion of the certificate program's first semester.)

- **IST 293—Studies in Network Security.** Provides an opportunity for students in multiple disciplines to discover and discuss a variety of issues related to security concerns in a computer network environment.

Current Implementations at Anne Arundel Community College

Anne Arundel Community College (AACC) in Arnold, Maryland, offers a scaled-down version of a certificate called a letter of recognition. AACC offers a systems security specialist letter of recognition for students completing nine credit hours of study.

The following two security courses are conducted under the auspices of the Computer Information Systems department (CSI), which offers this letter of recognition.

- **CSI 214—Information Systems Security** (3 credit hours)
  Introduces students to the protection of information and equipment in computer systems and associated communications networks. Topics include all aspects of systems protection, including physical security, hardware, software, and communications security. Includes a discussion and demonstration of issues related to recognizing and handling viruses. Addresses technical, legal, and ethical issues.

- **CSI 205—Cyberlaw** (3 credit hours)
  Introduces students to the emerging laws of cyberspace. Students explore methods of investigating and preventing cybercrimes and infringements on information security. Students discuss laws governing e-commerce and intellectual property protections, focusing on Napster and other cases. The class debates privacy rights and free speech on the Internet. (Also offered as CJS 205 in the Criminal Justice department.)

Course Implementations

Current Implementation at the Community College of the Air Force

The Community College of the Air Force (CCAF) is the largest multicampus community college in the world, with 122 affiliated schools and education service offices servicing 373,000 registrants—enlisted members pursuing their associate degree. The college offers a course titled Computer Systems Security as part of an information systems technology program of study. See the technical core requirements for this program in Table 3 or visit www.au.af.mil/au/ccaf/catalog/2002cat/ter_0iyy.htm for complete program requirements.

Table 3. Technical Core Requirements for CCAF's Information Systems Technology Program

Course Name	Max Credits
Airborne Information Systems	24
Broadcast Information Systems/Management	15
CCAF Internship	18
Command and Control Information Systems	15
Communications Networking	12
Communications-Electronics Program Management	12
Computer Systems Security	6
Data Information Systems/Management	20
Personnel Data Systems	12
Telecommunications Administration/Industry Regulation	6
Telecommunications Technology	6

Course Description

- **Computer Systems Security.** Addresses procedures for administering and monitoring automatic data processing security; security development, policies, duties, and responsibilities; system abuse; and establishment of security training programs.

CCAF also offers a course titled Informational Security as part of an information management program of study. See the technical core requirements for this program in Table 4 or visit www.au.af.mil/au/ccaf/catalog/2002cat/ter_1auy.htm for complete program requirements.

BEST COPY AVAILABLE

Table 4. Technical Core Requirements for CCAF Information Management Program

Course Name	Max Credits
CCAF Internship	18
Informational Security	3
Information Systems Administration	12
Information Systems Management	9
Microcomputer Software Applications	9
Office Equipment	3
Postal Operations/Management	15
Records/Publications Management	6

Current Implementations at Northern Virginia Community College

Northern Virginia Community College offers two security related courses as part of a certificate or A.A.S. degree in the administration of justice. For details about the program see www.nvcc.vccs.edu. The computer security course is an elective, while the information security course is required for both the certificate and the A.A.S. degree.

Course Descriptions

- **ADJ 157—Computer Security.** Examines security concerns with access controls, shutdown alternatives, hardware and software protection, and data encryption.

- **ADJ 256—Information Security.** Studies the means of protecting both government classified and private business information. Surveys techniques of storing, transmitting, destroying, and controlling access to sensitive information.

Current Implementation at Dallas County Community College District

The Dallas County Community College District in Texas offers a Web site system administration program that provides training in configuring, maintaining, and managing the server technologies used in the delivery of complex Web services. The program includes a network security course:

- **Network Security** (3 credits)
  Instruction in security for network hardware, software, and data, including physical security, backup procedures, firewalls, encryption, and protection from viruses.

BEST COPY AVAILABLE

Current Implementation at Anne Arundel Community College

Anne Arundel Community College (AACC) in Maryland offers both an A.A.S. degree and a certificate program in cybercrime. The following courses are offered through the Criminal Justice department:

- **CJS 205—Cyberlaw** (3 credits)
  Introduces students to emerging laws of cyberspace. Students explore methods of investigating and preventing cybercrimes and infringements upon information security. Students discuss laws governing e-commerce and intellectual property protections, focusing on landmark and other cases such as Napster. The class debates privacy rights and free speech on the Internet.

- **CJS 206—Cybercrime** (3 credits)
  Introduces students to technology-based crimes. Students explore cyber offenses including information warfare, cyber terrorism, information theft, data corruption, and disruption of service. Students discuss the computer as an instrument furthering the exploitation of children, acts of organized crime, and other criminal activities. Students identify vulnerabilities in national and private infrastructures, assess risks, and structure security measures. (Also offered as CSI 205 in the Computer Information Systems department.)

- **CJS 207—Cyber Forensics** (3 credits)
  Introduces students to forensic investigation of computer crime. Students explore a professional approach to investigating computer security incidents and learn to identify threats, create strategies to locate and recover evidence, and perform forensic analysis. Class discusses surveillance, tracing e-mail, and piercing anonymity through appropriate legal channels.

Current Implementations at Howard Community College

Howard Community College (HCC) in Columbia, Maryland, is planning to offer a three-credit course titled Management of the Virtual Private Network and Firewall as part of its training for Check Point certification. See the discussion of HCC in the following section.

Credential Program Implementations

Current Implementations at Edmonds Community College and Roane State Community College

Edmonds Community College (ECC) in Lynnwood, Washington, and Roane State Community College (RSCC) in Harriman, Tennessee, offer preparation for the Security Certified

Network Professional (SCNP) and the Security Certified Network Architect (SCNA) professional certifications conducted by Ascendant Learning (for details, see www.securitycertified.net/certifications.htm). The program descriptions at both institutions are nearly identical.

Edmonds Community College describes its Security Certified Program as designed for the IT professional who wishes to verify his or her skills as a security professional. ECC's SCNP program focuses on two areas of network security: firewalls and intrusion detection. The program is divided into two courses, Network Security Fundamentals (NSF) and Network Defense and Countermeasures (NDC).

- **Network Security Fundamentals.** This 48-hour course combines teacher-led lectures, in-class discussions, and hands-on lab exercises. The 10 domains covered in the course include such issues securing Windows, UNIX, and Linux operating systems; Advanced TCP/IP; security fundamentals; security implementation; router security; and attack methods. (Prerequisites: One of the following certifications or equivalent training or work experience: CCNA, CNA, CNE, CIW Associate, iNet+, MCP, MCSE, NETWORK+.)

- **Network Defense and Countermeasures.** This 40-hour course combines teacher-led lectures, in-class discussions, and hands-on lab exercises. The eight domains covered in the course include such issues as risk analysis, firewalls, intrusion detection systems, security policies, and virtual private networks. Almost 70 percent of the content is on firewalls and intrusion detection systems. (Prerequisite: Network Security Fundamentals.)

ECC's SCNA program is for students who want to take their security skills to the next level. Students learn how network security is moving toward trusted communication and how defensive schemes alone are not enough. The program deals extensively with public key infrastructure (PKI) and biometrics and is divided into two courses: PKI and Biometrics Concepts and Planning; and PKI and Biometrics Implementation.

- **PKI and Biometrics Concepts and Planning.** This 40-hour course combines teacher-led lectures, in-class discussions, and hands-on lab exercises. The six domains covered in the course include such issues as cryptography fundamentals, digital signatures, biometrics fundamentals, PKI fundamentals, PKI standards, and strong authentication. (Prerequisites: SCP Network Security Fundamentals and Network Defense and Countermeasures.)

- **PKI and Biometrics Implementation.** This 40-hour course combines teacher-led lectures, in-class discussions, and hands-on lab exercises. The six domains covered in the course include such issues as sign-on solutions, file encryption solutions, certificate server deployment, PKI solutions and applications, secure e-mail implementation, and network forensics. (Prerequisite: Network Security Fundamentals.)

Planned Implementation at Howard Community College

Check Point Educational Services
(www.checkpoint.com/services/education/aapprogram/index.html) has introduced the Check Point Authorized Academic Partner (AAP) Program Pilot to provide specialized VPN and firewall training as a stand-alone curriculum or as part of cybersecurity education programs in two- and four-year colleges. Check Point provides training and course materials for instructors teaching under the AAP program, which prepares students to sit for various cybersecurity certification examinations offered by Check Point (see www.checkpoint.com/services/education/certification/index.html).

Howard Community College (HCC) in Columbia, Maryland, is a certified Check Point AAP and is planning to offer Check Point Authorized VPN-1/Firewall-1 training as part of its network security curricula. The following course in network security is scheduled to be offered in the fall of 2002:

- **CKPT 210—Management of the Virtual Private Network and Firewall.**
  In this three-credit couse, students learn to define, administer, and troubleshoot an active security policy; improve VPN-1/FireWall-1 performance using a security policy; create network objects and groups; perform basic log management operations; configure anti-spoofing on the firewall; block intruders from accessing the network; set up user, client, and session authentication in a VPN-1/FireWall-1 environment; configure and set up network address translation (static NAT and hide NAT); back up critical VPN-1/FireWall-1 information; and uninstall VPN-1/FireWall-1.

Planned Implementation by CompTIA

CompTIA has drafted guidelines for a new Security+ certification program, which it describes as follows:

> Experts and industry leaders from all sectors of the IT industry, including training and academia, consulting firms, government, and other affiliated associations are working with CompTIA to develop the Security+ exam. This group of experts provides the resources and subject-matter expertise necessary to build a vendor-neutral, industry-defined security exam.

The exam, which is in its beta version as of this writing, will test five domain areas: general security concepts (30 percent); communications security (20 percent); infrastructure security (20 percent); basics of cryptography (15percent); and operational/organizational security (15 percent). The CompTIA Security+ foundation certification is expected to be a potential area of training by two-year colleges.

Summary

Community colleges across the United States can play a vital role in preparing professionals for careers related to cybersecurity. We urge faculty and administrators to use this report as a resource for initiating and expanding efforts in this area.

White Paper

8. IT Security Specialist—Integrating Academic Credentials with Professional Certifications

Neil Evans, Peter Saflund, and Manjari Wijenaike
National Workforce Center for Emerging Technologies
John Engman, Kris Madura, and Fran Linhart
CompTIA

Introduction

This paper discusses the integration of academic credentials and information technology (IT) professional certifications to infuse cybersecurity into all areas of IT education. Industry has divided cybersecurity specialists into a three-tier model:

Tier 1: Administrators—network administrators, technicians, and help desk personnel.
Tier 2: Engineers—bachelor's degree–level software engineers and developers.
Tier 3. Architect—master's degree– and Ph.D. level–system designers.

Community college academic credentials and IT professional certifications most directly impact Tier 1. Until recently, the infusion of cybersecurity skills into Tier 1 was a relatively neglected area. While the events of September 11, 2001, have heightened the importance of all levels of cybersecurity specialists, the industry was responding to the need for qualified Tier 1 personnel before that date. CompTIA leads a standards committee of industry leaders to develop Tier 1 certifications and competencies.

In February 2002, the U.S. Congress introduced a bill that would require federal agencies to follow a set of best practices to guard their computer systems. The Cybersecurity Research and Development Act of 2002 (H.R. 3394) will provide money to train more specialists in computer security. In its 2001 volume, *Building a Workforce for the Information Economy*, the National Research Council states that "finding people with the full suite of skills" [in the areas of computer security and data assurance is challenging].[1] In *Byte Wars*, Edward Yourdan discusses

[1] National Research Council, *Building a Workforce for the Information Economy*. Washington, D.C.: National Academy Press, 2001.

BEST COPY AVAILABLE

how all levels of IT professionals are encountering long-term changes in their jobs because they work in a world where cybersecurity is seriously considered in the implementation, installation, and architectural design of every computer system.[2]

The Demand for Cybersecurity Professionals

The rapid development of Internet, intranet, extranet, remote access, and mobile networking infrastructure technologies has left end users at all levels of the corporate structure demanding increased network access to greater amounts of information from multiple locations. This unprecedented level of network accessibility is being leveraged to enable all stakeholders (employers, customers, partners, and suppliers) to access internal corporate information and allow users to engage in e-business activities to purchase and transfer goods and services over the public network. As companies continue to build and expand their e-businesses, threats to networks increase, resulting in an increased need for security and a growing demand for skilled network services and security professionals.

The Computer Security Agency and the FBI issue an annual report on security trends and issues. The 2002 report confirms these emerging issues:

- Organizations continue to be under cyber attack from both inside and outside their electronic perimeters.
- Organizations have detected a wide range of cyber attacks. Seventy-four percent cite their Internet connection as the most frequent point of attack, while 33 percent cite their internal systems as the source of attack.
- Cyber attacks can result in serious financial losses as a result of the theft of proprietary information and financial fraud.
- Defending against cyber attacks requires more than just the use of information security technologies.
- Ninety percent of all respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months.
- Attacks on security occur despite a wide deployment of security technologies: 89 pecent of respondents have firewalls, 60 percent have an IDS, 82 percent have access control of some sort, and 38 percent use digital IDs.

According to Patrice Rapalus, director of the Computer Security Institute (CSI), these findings offer

> Compelling evidence that neither technologies nor policies alone offer an effective defense. Intrusions and theft of trade secrets takes place despite the presence of firewalls, encryption, and corporate edicts. Organizations that want to survive need to develop a comprehensive approach to information security, embracing both the human and techni-

[2] Edward Yourdon, *Byte Wars*. NJ: Prentice Hall, 2002.

cal dimensions. They also need to properly fund, train, staff, and empower those tasked with information security.[3]

Labor Market Data

Labor market data on security personnel are difficult to obtain because of the wide variety of job classifications that have security duties incorporated into them. In a survey of 302 organizations across several industries conducted by the Computer Security Institute, staffing for information security was anticipated to increase 14.86 percent in the coming year and the annual budget for information security overall was expected to increase 20.42 percent. The average salary paid to information security staff members, across all industries, was $88,424. The health-care industry spent by far the most per information security worker, and educational institutions spent the least.

> In spite of the trend towards the use of sophisticated technical tools rather than people to perform certain security functions, and in spite of the trend towards the empowerment of users and others to attend to their own information security needs, the relative number of staff with assigned information security duties is growing at a significant rate. (Computer Security Institute, 2002)

A Foote Partners' salary survey of security workers cited in *Information Security* magazine (September 2001) found that pay raises for security practitioners continued to outstrip other IT job categories, especially for practitioners with specialized skills or professional certifications. The survey found that technical certifications for security were viewed positively by employers and regularly factored into compensation, selection, and promotion decisions.

Security professionals will need to diversify their skill sets to maintain higher pay levels. While continuing to master new technologies for protecting IT systems, they will be under more pressure to understand their companies' businesses and pinpoint the security risks that most threaten their companies' bottom line.

The Foote Partners survey anticipates that growth in security skills and certification pay will continue to accelerate, routinely beating the overall growth rate for skills premium pay. Security-related salaries will continue to substantially outperform overall IT compensation as a result of

- The inclusion of basic network engineering and operations skills into security jobs regardless of specialization.
- Rapid growth in new security niches—for example, forensics and intrusion detection.
- New technologies with broad appeal (for example, Microsoft's XP and .NET).
- The continued supply-and-demand gap for security professionals (one of the widest in any IT job category).

[3] 2001 Computer Crime and Security Survey, Computer Security Institute, March 12, 2001.

The survey predicted that the ability to do the following security tasks will be highly valued over the next 12 to 24 months:

- Comply with new security and privacy regulations in health care and finance.
- Develop stronger user-awareness policies.
- Address security issues pertaining to wireless access, business-to-business exchanges, and application service providers (ASPs).

While knowledge of the technical side of security is obviously important, critical success factors for security professionals will also include being adept at corporate politics; possessing business skills and aptitudes; having good relationship management; and being able to market, sell, and negotiate outcomes.

Who Is the Cybersecurity Worker?

The cybersecurity worker's role in the workplace is not clearly defined. Some industry organizations have and continue to evolve a security workforce, but up until recently such organizations have typically been consulting firms or security-specific organizations. Throughout most of industry, security responsibilities have typically fallen upon non security workers, such as the network administrator who has security responsibilities and is responsible for some aspects of network security. Not until 2001 did industry, particularly in organizations with less than 10,000 employees begin to recognize that security is a necessary separate unit. The skills and responsibilities described by a title (administrator, engineer, architect) in one organization do not necessarily match the skills and responsibilities described by the same title in another organization.

It is clear that security organizations are seeking qualified security professionals, as it is no longer acceptable to buy a firewall package, install it, and let it run. The certified security professional must know what is being protected and what value it has, both perceived and real. The individual must recognize the potential from inside the network for either intentional or accidental violation of data flow, and understand all avenues of defense and which are applicable to each attack situation.

According to Rebecca Herold, a consultant with Netigy,

> Protecting networks and information is a vital component for the success of a business but too many companies still give these security responsibilities to staff who are not qualified or do not have the appropriate background. Companies need to budget for high quality information and network security staff...the days of placing personnel into positions labeled "security" that have no influence over security direction and only spend time doing data entry into access control databases at the direction of programmers, secretaries, clerks, and other positions within a company has got to come to an end.[4]

[4] Rebecca Herold, consultant with Netigy (www.netigy.com).

To illustrate the need for training in broad security practices, it could be argued that having a security professional who is certified on one particular type of firewall is like having a security guard whose only responsibility is to lock the front door and watch the lock. The guard would pay no attention to the other doors, windows, ceilings, and so on.

Where do organizations find cybersecurity personnel with the right training and skills? If a company identifies a potential candidate, how can it verify the education, experience, or certifications the candidate claims to have? In building a qualified workforce, it is critical that security professionals have a solid, well-rounded knowledge of security and security principles backed up by experience and industry certification.

Trends of Cybersecurity Credentials and Educational Programs

Since the events of September 11, 2001, two- and four-year colleges, universities, and other private educational institutions have responded rapidly to heightened awareness that the U.S. is in urgent need of cybersecurity (a.k.a. information and data assurance) professionals.

This section discusses the current best practices of community colleges in meeting current demand for security skills. It also projects future demand for IT workers with security skills and presents some actions that community colleges might take to respond to this demand. Several trends in IT security workforce development and education programs frame an appreciation of how community colleges view the current and future demand for IT workers:

- The majority of students requiring security skills will come from two main groups: current and future preparatory students (enrolled as IT majors seeking employment in IT after graduation), and practicing IT technicians, engineers, and architects who are adding to their knowledge and skills base.
- The majority of community college IT students are (or will become) employed in IT career clusters as defined by CompTIA and the National Workforce Center for Emerging Technologies (NWCET) through an industry-driven national skill standards project in 2002.
- Community colleges may serve a vital role in preparing students for advanced (professional and master's degree level) certification in security areas.
- Few if any two-year graduates will have cybersecurity as a full-time job. Rather, they will integrate new security skills into their customary job roles and daily duties.
- There is an obvious need for cybersecurity designers and architects at the master's degree and Ph.D. levels. Overarching national interests also demand cybersecurity technicians who are skilled in application, integration, system monitoring, forensic analysis, deterrence, and user education.

From both a workforce development aspect and a practical implementation perspective, the role of community colleges in education and certification should not be underestimated. Community and technical colleges serve three related but distinct missions in cybersecurity:

- Preparing emerging workers to enter traditional IT job roles with IT security skills.
- Assisting incumbent technicians to gain required security skills.
- Ensuring that transfer students acquire appropriate SMET (science, math, engineering, and technology) skills to succeed in undergraduate and graduate university programs that prepare Tier 2 and Tier 3 personnel.

Many cybersecurity offerings are available at the master's degree and Ph.D. levels to students who wish to pursue this educational pathway. Notable examples of program offerings at these levels include programs at Purdue University, where the National Science Foundation (NSF) is funding scholarships for students pursuing a master's degree in computer security who make a commitment to work for the federal government; George Washington University, which offers master's and Ph.D. focus programs in computer security and information assurance; and Idaho State University. These three institutions are National Security Agency (NSA) Centers of Academic Excellence in Information Security. The reason for the large number of cybersecurity programs at the master's and Ph.D. levels is that until recently cybersecurity was viewed by academia as a largely architectural and design issue, rather than as an issue of technician-level skills involving implementation and enforcement.

Two- and four-year colleges are fast becoming players in this arena. NWCET's host institution, Bellevue Community College in Bellevue, Washington, is in the process of integrating cybersecurity course modules into its computer science programming and networking tracks. Norwalk Community College in Connecticut successfully partnered with a four-year institution, Western Connecticut State University (WCSU), to create a degree program in computer security.

Cybersecurity Faculty Development and Recruitment

A critical obstacle for most two- and four-year colleges as they strive to develop program and credentialing opportunities in cybersecurity is the recruitment and professional development of skilled faculty. Although they do not provide the advanced degrees required for research-oriented and advanced cybersecurity careers, the nearly 1,800 comprehensive community and technical colleges in the U.S. and the more than 15,000 IT faculty teaching courses in these institutions can and will play a significant role in the improvement of cybersecurity education by expanding the pool of security-savvy IT professionals at all levels. Corey Schou at Idaho State University believes that undergraduate programs may "have the largest potential influence" on the current shortage of security personnel. He argues that "more undergraduates can be produced with fewer resources" and "undergraduates immediately enter the job market as practitioners."[5] In other words, cybersecurity is not the exclusive province of either designers or technicians; both play a necessary role.

Significant improvements in faculty development and recruitment will be required to ensure that community colleges can provide fundamental and advanced skills at the applied level.

[5] Corey Schou, "Information Assurance Education—A Worldwide Security Crisis," *Syllabus*, August 2001.

Not only is the shortage of community college instructors particularly critical in this relatively new field, existing and newly hired faculty must be aware of the contextual factors and realities of cybersecurity issues at the point of implementation. The NSF's evaluation center at Western Michigan University finds that "the traditional professional development model for educators is inadequate to meet the existing need for technology training among community college faculty."[6] Community college faculty must have the ability to integrate components of cybersecurity into their existing and future technician-level IT curricula and must have the tools and skills necessary to teach these components. The NWCET's Educator-to-Educator Institute is currently working on this issue and developing Cyber-Security modules to provide community college educators with timely and high-quality professional development opportunities. CompTIA, through its JOBS+ program, works closely with community colleges nationwide to transmit timely industry information and standards to both students and educators and will incorporate opportunities for educator training around its Security+ certification.

Best Practices in Curricula, Courseware, and Course Materials

With respect to curricula and courseware development in cybersecurity, educators have to operate on the premise that Tier 1 workers are as crucial as Tier 2 and Tier 3 workers. This group is a key component in proper installation of software and hardware, user education, and daily monitoring of systems. These functions must occur in a design context that is transparent to users, and that is where higher-level degrees in cybersecurity come into play. Before September 11, 2001, business and government were both able to make choices about levels of security implementation and design in terms of time and cost. Such choices are no longer an option. Now, community colleges are in the forefront of preparing at least two types of IT workers who figure prominently in cybersecurity decision making processes: IT-related managers (for example, operations managers, Web site managers, and finance managers) and IT technicians.

While cybersecurity programs, especially at the two- and four-year levels, are in their nascent stages, a few excellent sources of curricula, courseware, and course materials that span the entire K-12 spectrum are available nationally. For example, Purdue's Center for Education and Research in Information Assurance and Security (CERIAS) provides K–12 educators with classroom materials, Web-based resources, and teacher-generated lesson plans to teach information and computer security.

The NWCET hopes to play a vital role in the community college's development of cybersecurity curricula and courseware, and it recently received a grant from NSF to develop cybersecurity skill standards by fall 2002. Educators will be able to use the newly created standards as a foundation for curriculum and courseware development on a national scale.

[6] Norman Gold and K. Powe, *Assessing the Impact and Effectiveness of Professional Development in the Advanced Technological Education Program*. Kalamazoo, MI: The Evaluation Center, Western Michigan State University.

Strengths and Weaknesses of Academic Credentials

The strengths of academic credentials in IT cybersecurity are manifold and prepare a student for lifelong achievement. Having accredited academic credentials in this area allows a student to set a long-term goal, work hard to achieve that goal, be measured at critical points with appropriate assessments, and obtain a degree. This process is focused on principles and concepts rather than on specific job skills and technical hands-on know-how.

On the other hand, academic IT credentials frequently lack the currency and market relevance of IT certifications. They do not necessarily recognize past IT certifications or prior experience. In addition, they are not based on outcomes or based on industry-driven skill standards, and for many students who are also working professionals, traditional degree programs take too long.

In all areas of IT, but especially in the time-critical area of cybersecurity, it is important to create educational programs that are not only based on skill standards but also have IT certifications built in as part of a career and educational program or pathway.

IT Professional Certifications

According to a study conducted by IDC, the following are the most significant trends recently observed in the certification market:

1. IT certification sponsors are increasingly choosing to endorse, articulate to, or acquire existing certification programs instead of building their own, especially for entry-level credentials. For example, Novell, Microsoft, and Intel have eliminated certifications, training, or entire programs in favor of adopting CompTIA certifications that lead to or are incorporated into their certification programs.
2. The use of and preference for role-based certifications is increasing. The majority of certified IT professionals hold certifications related to the following job roles:

    - General IT technician (34 percent)
    - Network administrator (18 percent)
    - Network engineer (17 percent)
    - System administrator (16 percent)
    - Web professional (11 percent)

The fastest-growing job role certification areas are for database professionals, network engineers, application developers and programmers, and computer and network security personnel. Web professional certifications grew at a slower pace than anticipated.

Although the IT certification programs offered are split almost equally among entry level, intermediate, and advanced, the majority of certifications granted are for entry-level and intermediate positions.

The following factors are likely to continue to drive IT certification market growth:

- With the emergence of IT technologies such as wireless, data/voice integration, and security, the demand for related skills and for certifications to validate these skills will increase.
- The persistence of a significant IT labor shortage despite economic slowdown will drive growth. Certification will help bridge the gap and can play a role in training new entrants and career changers for IT jobs, as well as in maintaining and retaining the existing talent pool.
- The adoption of certification by individuals as part of a lifelong learning process will be a driver. Workers are increasingly being forced to take control of their careers in a continually competitive workforce.
- The adoption of certification by corporations as part of their investment in human capital will increase growth in this market. Corporations are becoming increasingly aware of the benefits of certification in the form of increased productivity and services improvement.
- The globalization of the IT market will continue to grow regionally in markets outside North America.

The Role of Skill Standards and Certifications

Certifications of varying types will apply to all three tiers of the model described in this paper. For cybersecurity system designers and architects, certifications may mirror other advanced professional-level certifications and thus be similar to a board certification in medicine, or a Professional Engineer or a Certified Public Accountant qualification. Advanced professional certification might require extensive exam preparation and experience similar to a medical residency or Engineer in Training (EIT) training.

For technicians, managers, engineers, and developers, certifications may be tailored more toward verification of specific applied skills, again conforming to practices already in place for these occupations. These certifications could range broadly, however, from verification of basic skills similar to CompTIA's A+ to technological certifications like Microsoft's MCSE or Cisco's CCIE.

Skill standards are the perfect compass for charting the course of security certifications. Since they are industry based, certifications based on skill standards will accurately reflect current needs and can be rapidly adapted to meet changing requirements.

Skill standards also offer the advantage of providing a platform for integrating certifications into the more complex mosaic of professional credentials, and they provide a basis for determining equivalencies between certifications and college or university coursework or corporate training. Because they make the rungs in a career progression ladder visible, skill standards can be used to define career and skill attainment benchmarks. Thus, skill standards serve as a reference point upon which conventional education, training, and certification can converge.

Certification may prove to be the most efficient pathway for existing IT professionals at every occupational level to verify that they have acquired the desired skills and knowledge in the emergent area of cybersecurity. Standards-based certifications can also provide educators with a quick way of identifying what content areas need to be enhanced or added to current IT programs. They can also give both new and incumbent workers a map for effective planning of future career progression.

Available Cybersecurity Standards and Certifications

IT companies that support cybersecurity certification have no desire to provide higher education. Certifications do not replace experience or degree programs. They *do* reflect the current state of knowledge and practice, and as such can serve as acknowledgement of and proof that a job candidate who holds certification possesses a body of current knowledge and skills.

There are now three types of security certifications:

- **Industry Sponsored Vendor-Neutral Certification.** Not-for-profit organizations like CompTIA, SANS, and ISSP host the development of vendor-neutral certifications. The content and goals of these and their exams vary. The exams can be foundational in nature (CompTIA's Security+), technology specific (SANS certification targeting firewalls, intrusion, and forensics), or at a higher level of expertise (CISSP's portfolio-based exam designed for candidates with a minimum of four years of experience). In the case of CompTIA's Security+ certification, more than 30 corporate, government, and academic organizations came together to define and document the target candidate and job role of the Tier 1 security worker. These organizations donated over 10,000 subject matter hours to research and build the Security+ exam. The results of this research are in the public domain, available on CompTIA's Web site (www.comptia.org). See Table 1.

- **Vendor-Specific Certification.** Vendor certification programs designed to train qualified workers in vendor-specific skills and knowledge are used to ensure that trained workers are available to support the product or technology in the field. Vendors are committed to identifying and training quality staff: the more qualified the technical team is, the better the product will function. Many vendors (such as Entrust, RSA, and VeriSign) recommend or require that the candidate pass a foundational exam like Security+ prior to taking the vendor's exam program. See Table 2.

- **Training Company Certification.** Training companies can produce and market an exam that is based on curriculum, written by instructors or subject matter experts. See Table 3.

Table 1. Vendor-Neutral Certification

Organization and Certification	Level	Training	Development
CompTIA (Computing Technology Industry Association) **Security+ Certification Exam** 90-minute multiple-choice exam available September 2002	Foundational exam for Tier 1 security workers. No exam prerequisites; 12 months of network experience recommended. Test takers include: • Network administrators • System administrators • Help desk specialists • DB administrations • Firewall analysts • System analysts • Security specialists • Security administrators • Information assurance specialists • IS security specialists	CompTIA does not produce training content. Research results (Job Task Analysis) will be published November 2002. Preliminary information is available on the Web. Curriculum that maps to the job role and test objectives can apply for and receive the **CompTIA CAQC** logo. Certain security vendors will require the Security+ exam prior to enrollment in their vendor-specific tracks.	The exam is developed and maintained in compliance with industry standards (AERA, CLEAR, APA, NOCA). The governing committee for Security+ includes • **Government**: NIST, NSF, Cybersmuggling Center (U.S. Customs), Argonne National Laboratory (DOE), and other government agencies. • **Training**: Marcraft/Pearson, Course Technology, Intense School, Ascendant Learning, Tech Connect, Guru Labs, Sybex, Element K, New Horizons • **Manufacturers/Distributors**: VeriSign, Olympus Security Group, Institute for Excellence in Information Technology, RSA Security, Sun Microsystems, Entrust, Microsoft, IBM/Tivoli Software, KPMG, CheckPoint, Cisco, Motorola, BMC Software, EDS, Internet Security Systems, Computer Science Corporation

BEST COPY AVAILABLE

Table 1. Vendor-Neutral Certification (continued)

Organization and Certification	Level	Training	Development
(ISC)² International Information Systems Security Certifications Consortium, Inc. 1. **CISSP** – Information systems security professionals; and 2. **SSCP** – Information systems security practitioners	***Higher-level exam*** Candidates must demonstrate a minimum of 3 years experience in one or more of the domains of the Common Body of Knowledge [available through (ISC)²]. As of 1-03, the experience required will be four (4) years, or three (3) years with a college degree from an accredited college or university.	(ISC)² has developed curriculum based on their Common Body of Knowledge for IS security professionals and practitioners. These curriculum materials include a Study Guide and Review Courses.	The examinations are developed, maintained, administered, and scored in compliance with key testing industry standards [the most important of which are promulgated by the APA, NCME, AERA, the federal government (EEOC), CLEAR and NOCA], to ensure the integrity of the measurement process.
GIAC.ORG Global Information Assurance Certification SANS	***Technology-based exams*** covering: • Security Essentials • Firewall Analyst • Intrusion Analyst • Incident Handler • Windows Security Administrator • UNIX Security Administrator • Information Security Officer–Basic • Systems and Network Auditor • Forensic Analyst • Security Leadership	Each GIAC certification is designed to stand on its own, and represents mastery of a particular set of knowledge and skills. There is no particular "order" in which GIAC certifications must be earned. Multiple courses available. Course content/curriculum parallels exams.	The GIAC Advisory Boards are made up of GIAC certified individuals who take an active role in the GIAC program. Participation is voluntary; GIAC professionals who receive "honors" on their practical assignment or a 90 or better on one or more of their exams are eligible for membership on the Advisory Board for their certification.

BEST COPY AVAILABLE

Table 2. Vendor-Specific Certification

Vendor	Certification	Training
Baltimore	No certifications	20 courses
Check Point	Security administrator (CCSA) Security engineer (CCSE) Addressing engineer (CCAE) Quality of service engineer (CCQE)	Training parallels the exams
Entrust	Entrust RA Specialist Entrust Consultant, where RA Specialist is a prerequisite	Training parallels the exams
ISS (Internet Security Systems)	10 exams	10 training programs
RSA	3 certification levels CSE – engineer CA – administrative CI – certified instructor	3 training programs
Symantec	3 certification levels Certified Professional (SCP): Pass one exam Certified Security Engineer (SCSE): pass 3 tests Symantec Certified Security Consultant (SCSC) higher level	Training parallels the exams
TrueSecure	ICSA – architect ICSE – engineer	Training parallels the exams
VeriSign	3 certification levels VCA – administrator VCE – engineer VCPE – professional engineer	Training parallels exams VCA = 3-day course VCE = 5-day course VCPE = 10-day course

Table 3. Training Company Certification

Training Company	Certification	Training
CIW	Security Professional	5-day training program
Security Certified Program	Security Certified Network Professional	

BEST COPY AVAILABLE

Strengths and Weaknesses of Cybersecurity Certifications

Certification has evolved to become an agreed-on unit of measure for specific knowledge and expertise about a particular product or technology. Formal training has long been a preferred method for IT technical staff to learn about a particular product or technology. Certification is used to assess the degree of competency developed through the training. Training may be characterized as the investment in product or technology competency, while certification is the measure of impact derived from this investment. Certification is a means to assess the return on investment from training dollars spent.

Several studies on the value of IT certification (Dataquest, IDC, Gartner) reveal the growing industry demand and confidence in both vendor and vendor-neutral training and certification. Both managers and peers regard certified professionals as highly credible, productive team members. Additionally, IT professionals are increasingly using technology training courses and certification to stay on top of current and future innovations.

IT managers frequently cite cost and turnover as drawbacks to introducing training and certification into their organizations, although research indicates that certified workers are no more likely to leave an organization than noncertified employees are. Dataquest found that certified employees will stay with an employer longer than those who have not received certification, and fewer than one out of 10 managers say that certified employees are more likely to leave.

In the Gartner study, 64 percent of managers cite a higher level of service as a key benefit of having certified staff, followed by a competitive advantage (59 percent) and increased productivity (57 percent). Other benefits include simplified recruiting and hiring processes. Among managers, the benefits of certification outweigh the drawbacks by 3 to 1.

From a candidate's perspective, the benefits of being certified are increased credibility within the organization, higher compensation, more credibility with customers, and an improvement in problem-solving skills. The observation of increased credibility and compensation is somewhat at odds with managers who claim that they do not value certification, and may lead to the belief that managers may increase compensation based on productivity or other improvements as a result of certification rather than the mere fact of an employee being certified. The Dataquest study found that, on average, managers are willing to pay a 10 percent premium for certified employees.

The number of cybersecurity certifications is growing and can be divided into those that measure in-depth training in a particular technology or vendor product, those that offer relatively expensive multitrack approaches, and those that are focused on senior policy development and general security management. Very few organizations, with the exception of CompTIA, are developing certifications that provide a foundational set of skills that prepare the employee for a wide variety of job roles and security technologies.

As certification programs evolve to meet the challenge of practical expertise vs. textbook knowledge and as new technologies continue to change, perhaps the only feasible measure of an individual's expertise will be an industry- or vendor-defined certification.

Though it is a small, emerging segment of the IT certification industry, the security area is experiencing significant growth rates and will most likely remain a hot certification topic in the near future. Cybersecurity certification will, like IT certification in general, evolve to become a critical differentiator for the individuals who attain certification and the companies that employ them.

Building Skill Standards and Certifications into Educational Programs

Skill standards in cybersecurity and the industry research behind IT certifications such as CompTIA's Security+ will provide the material and matrices necessary for a consistent evaluative framework, putting all eligible sources for proving knowledge on a single, visible footing. Such an evaluative framework will take into account experience, corporate training, previous knowledge, training, and certifications, which will be included in an overall academic credential.

Summary

The development of cybersecurity skill standards and industry-driven certifications will establish cooperation among government, industry, and education to stay current with requirements in this area. As national interests and awareness grow, they will affect current and future government policy, making skill standards and certifications a framework with which to gauge and measure future educational developments in this field.

White Paper

9. Adapting Commercial Training Materials for Use at the Community College

Erich Spengler and Aurora Zwick
Moraine Valley Community College

Introduction

In the aftermath of September 11, 2001, federal, state, and local governments are making rapid changes in security preparedness in order to prevent potential terrorist attacks on financial institutions, databanks, and information systems across the country. It is urgent that academic, government, and commercial institutions begin new and effective training initiatives to combat the threats of such attacks. Many colleges have partnered with businesses to perform needs analysis and develop specific job classifications for critical cybersecurity positions. They have found that knowledge and skills are needed in the following security areas:

- Virtual private networks
- Firewalls
- Public key infrastructures
- Vulnerability testing and assessments
- Role and responsibility of local, regional, national authorities
- Security awareness and best practices
- IT forensics
- Basic criminal law
- Penetration testing
- Security devices (retinal scanners, smart cards, etc.)

The purpose of this paper is to share ways that community colleges can adopt curricula and partner with vendors to develop comprehensive information technology (IT) security programs. This paper identifies *models, strategies, and instructional partnerships* used by Moraine Valley Community College of Palos Hills, Illinois, and other two-year institutions to leverage the training products and related materials produced by several of the largest companies in the IT security market in college degree and certificate programs.

BEST COPY AVAILABLE

Models for Adopting Curricula

One of the more common obstacles that prevent many community colleges from establishing effective technical training programs is the expense of developing new curricula. There are several models that can be used to integrate existing commercial curricula into college vocational and degree programs. In developing technical curricula, community college faculties have documented vast differences in the way companies approach training partnerships with academic institutions. Although companies recognize the value of their products and educational materials being used in the academic environment, many still find the technical training capacity of community colleges to be a threat to their own commercial training divisions. This paper discusses three models that two-year colleges have used in adopting commercial IT curricula.

Mutual Partnerships Training Model

Mutual partnerships represent the highest level of cooperation between commercial partners and academic institutions. These programs are typically initiated and financed by corporate partners to develop instructional materials, training products, and real-world case studies. Corporate partners may also provide affordable instructor training and product packaging to academic partners. The academic institutions provide the corporations with many benefits that are not typically realized by commercial training avenues, including

- Larger and more diverse audiences
- Outreach to underrepresented populations
- Affordable training programs that are directed toward the entry-level employment pool
- Establishment of teaching and learning standards
- Academic credentials
- A greater exposure of products and technologies

Companies including Cisco Systems, Sun Microsystems, and Microsoft Corporation have launched worldwide training campaigns with universities, community colleges, and high schools. These programs have resulted in high-quality standardized curricula that can be afforded by many academic institutions. With an increased number of trained professionals, these companies have been able to lower the total cost of product ownership. This is achieved by decreasing end-user training costs and increasing the pool of qualified IT professionals. Additionally, these training programs are tied to certification programs, which helps to ensure effectiveness and consistency of instruction.

Independent Vendor/Certification Training Model

The independent vendor certification training model is based on academic institutions adopting and developing independent instructional materials built upon the commercial training materials and/or product certification standards. IT curricula and training vendors view this as a direct threat to their own bottom line. Many vendors create academic train-

ing programs that institutions can not afford given state and local tuition structures. For many academic institutions, adopting proprietary corporate training programs is not economically feasible. The programs may also impose and enforce restrictions on material usage and delivery schedule. These obstacles have forced many colleges to develop their own training programs, based on commercially developed training standards and objectives, to prepare students for product and industry certifications. These programs can be very difficult and extremely costly to implement. However, many have proven to be more effective than the corresponding commercial training programs. One of the benefits of this model is that it results in targeted training materials that can be modularized and customized for instructional delivery. The flexibility of this model enables academic training intuitions to adapt the curriculum to more varied audiences.

Vendor-Neutral Training Model

Many emerging information technologies have diverse market share. An academic institution that provides training in one of these IT areas needs to address a wide range of product options and applications. As a result, a single survey course may teach students how to use several competing products, providing an overview of each; comparing the features, strengths, and weaknesses of the products; and discussing the best applications for each product. Many of the companies that produce the products in question contract with third-party vendors to provide training in their products. These training vendors are usually interested in product exposure and may offer a great opportunity for low-level local partnerships. They may depend on their academic partners to provide needs analysis and curriculum development. This model maximizes student's exposure to technologies and to the product selection process as well. Under this model, it is difficult to keep curricula current with product trends and market share; locate competent instructors with the necessary background in diverse products; and afford the cost of equipment, training, and support.

Table 1. Three Models for Adopting and Developing IT Training Curriculum

Mutual Partnerships
Advantages • Needs and skills analyses and the curriculum development process are performed and financed by the commercial partner • Standardization and quality assurance ensure better articulation • Implementation timeline • Instructor training and certification program • Evaluation and assessment • Lab requirements and equipment selection
Disadvantages • Not vendor neutral • Delay in alignment to industry products and vendor certifications • Academic institution's contract reluctance • Control over usage of curriculum • Instructor qualification requirements vs. local union contracts • May not meet local needs • Not customizable • Ownership • Dependence on vendor's success
Independent Vendor and Certification Training
Advantages • Programs are indepent because they are owned by academic institution • Flexibility of delivery time • Course material and textbook selection independence • Lab design and equipment selection independence • Customization
Disadvantages • Cost and time to develop materials • Retooling of curriculum to match ongoing certification requirements • Comprehensive approach to technologies • Higher dependence on faculty product knowledge and certification maintenance • Difficult to identify and establish standards
Vendor-Neutral Training
Advantages • Comprehensive approach to technology training • Vendor neutrality • Partnerships with corporations and training vendors • Addresses local market needs • Modularization and ownership • Flexibility of delivery
Disadvantages • Cost of curriculum development process • Higher dependence on faculty product knowledge and certification maintenance • Standardization and quality assurance • Difficult to maintain curriculum current with product life cycles

BEST COPY AVAILABLE

Overview of Three Partnership Programs

Here are brief overviews of the IT training programs that three commercial vendors provide in partnership with academic institutions.

Microsoft IT Academy Program
The Microsoft IT Academy Program is an alliance between academic institutions and Microsoft. The joint mission is to deliver a premium education on cutting-edge Microsoft technologies.
1. **Academy Obligations** Academy hereby agrees to comply with all of the terms and conditions contained herein as well as all requirements as set forth in the Microsoft IT Academy Program Guide ("Program Guide"). In addition, Academy agrees to provide training according to the following guidelines: 1.1 All training on Microsoft products will be based on the printed and online course materials which Microsoft has developed relating to systems, support, and developer training for computer professionals, including but not limited to trainer-led course materials, online course materials, and Microsoft self-paced course materials ("Microsoft Official Curriculum" or "MOC"), or on the Microsoft Press Academic Learning Series ("Microsoft Press Academic Learning Series" or "ALS") as more fully described in the Program Guide. Academy may use non-Microsoft supplemental materials and content ("Supplemental Materials") whenever appropriate. Supplemental Materials exist for the relevant product. Except as otherwise provided in the Program Guide, Academy shall **ONLY** be entitled to purchase MOC for use by students corresponding to courses for which the Academy has a certified instructor. Members may purchase MOC instructor kits any time after receipt of the Notice of Acceptance e-mail. Level II members may purchase MOC for use by students for courses taught by a Microsoft Certified Professional ("MCP") retained by such member for a product on which such MCP has not yet been certified on a one-time-only basis. **MOC may not be copied, duplicated, or otherwise reproduced.** 1.2 Except as otherwise provided in the Program Guide for Level II members, training shall only be delivered by instructors who are certified as an MCP for the product that is the subject of training. 1.3 Training shall only be delivered to students who are officially enrolled in Academy for credit or non credit instruction. 1.4 Except as otherwise provided in the Program Guide, training courses, including instructor monitored or facilitated lab time, may not exceed twelve (12) hours per week. Training provided to faculty members is exempt from this twelve-hour rule.
2. **Payment** Payment of the annual subscription to the Microsoft IT Academy Program may be made via credit card or purchase order. In order to use a purchase order, Academy must either submit a credit application at time of program registration, or have been a Microsoft Authorized Academic Training Provider ("AATP") with a current credit application on file for the purpose of purchasing MOC materials. Payment of the annual subscription fee of U.S. $5,000 (Level I membership) or U.S. $1,500 (Level II membership) must be received by Microsoft within thirty (30) days of the Academy's receipt of the Notification of Acceptance e-mail. Any amounts more than sixty (60) days past due shall constitute a material breach of the Agreement and shall entitle Microsoft to immediately suspend all benefits until payment is received or terminate Academy's membership. All membership fees must be paid in U.S. dollars.

BEST COPY AVAILABLE

Cisco Networking Academy Program
The Cisco Networking Academy Program (CCNA) is a comprehensive e-learning program, offered in 10 semesters, that provides students with the Internet technology skills essential in a global economy. The Networking Academy program delivers Web-based content, online assessment, student performance tracking, hands-on labs, instructor training and support, and preparation for industry-standard certifications. Launched in 1997, there are now over 7,500 Networking Academies in over 130 countries and in all 50 U.S. states. Over 160,000 students are enrolled in Academies in high schools, colleges and universities, technical schools, community-based organizations, and other educational programs around the world.
Types of Academies and Their Responsibilities There are three types of academies: Local Academies, Regional Academies, and Cisco Academy Training Centers (CATCs).
Curriculum The online portion of the curriculum contains eight 70-hour blocks of study called semesters, which total 560 hours. High schools/secondary schools typically teach the CCNA (semesters 1–4) in two academic years, whereas colleges and universities typically use one academic year to deliver the entire CCNA curriculum. The curriculum is copyrighted. Access to the curriculum should be provided only to students enrolled in Networking Academy classes and IS personnel within the institution offering the program. Appropriate firewalls to protect this information from unauthorized access are required. Academies may not copy, directly or indirectly, Cisco published materials (including Web pages), or any part of the text, graphics, logos or trademarks from Cisco's published materials or engage in distribution of Cisco's copyrighted material. Further, schools are not allowed to develop courseware that is substantially similar to the four-semester online curriculum, nor are they allowed to state or imply that the curriculum is anything but Cisco's property. [10.20.99]
Equipment Cisco donates refurbished lab equipment to Regional Academies and to CATCs. Cisco also donates lab equipment to schools in officially recognized Empowerment Zones. Currently, both donated and purchased labs include 5 routers, 2 LAN switches, software, cables, and first-year product support. [02.14.99]
Instructor Training Regional Academy instructors are trained by Cisco Academy Training Centers offering the CCNA curricula (CATC-CCNAs). Semester training lengths are as follows: • Semester One = 5 Days • Semester Two = 6 Days • Semester Three = 4 Days • Semester Four = 4 Days

BEST COPY AVAILABLE

Check Point Authorized Academic Partner (AAP) Program

Check Point Education Services is proud to announce the introduction of its Check Point Authorized Academic Partner (AAP) Program Pilot.

This program has been designed to work with colleges and universities to offer Check Point training as part of two- and four-year degree programs worldwide. Its main focus: to provide quality security education to degree-seeking students.

Participation in this program provides academic institutions with the best tools to easily integrate Check Point Authorized VPN-1/FireWall-1 training as part of their existing security curricula. For those colleges and universities that do not already have a security program or courses, the Check Point AAP program gives them the training and tools necessary to begin teaching a solid security course.

Objectives:

- Provide a global program
- Provide training as part-degree programs (2–4 year degree program)
- Create structure to benefit Check Point, Partners and Students
- Integrate into the Check Point Services Partner Program
- Encourage academic students to prepare for and obtain certification
- Provide scalable structure for expansion into e-learning
- Create an easy to implement program for integration into existing Computer Science Technology programs
- Recognize an untapped education market

IT Security Standards and Certification Organizations

In addition to commercial and product training, there are several industry training standards and certifications that can be combined to form a valuable resource in the curriculum development process. These organizations offer vender-neutral certifications. Many two-year institutions are basing their certification standards on ISC, SANS, and CompTIA.

International Information Systems Security Certification Consortium, Inc.

$(ISC)^2$ is a global, not-for-profit organization dedicated to

- Maintaining a Common Body of Knowledge for Information Security [IS].
- Certifying industry professionals and practitioners in an international IS standard.
- Administering training and certification examinations.
- Ensuring credentials are maintained, primarily through continuing education.

Governments, corporations, centers of higher learning, and organizations worldwide demand a common platform for and proficiency in mastering the dynamic nature of information security. $(ISC)^2$ helps fulfill these needs. Thousands of IS professionals in over 60 countries worldwide have attained certification in one of the two designations administered by $(ISC)^2$:

- Certified Information Systems Security Professional [CISSP]
- System Security Certified Practitioner [SSCP]

BEST COPY AVAILABLE

CompTIA
CompTIA (Computer Technology Industry Association) helps shape the technology community with programs that set both present and future standards and guidelines. As a participant in these activities your company will work with partners, potential partners, and competitors to influence and advance every facet of the technology community. CompTIA gives you a voice and provides a vital link to major segments of the technology markets. CompTIA is hosting and sponsoring the development of a non-vendor-specific industry-supported security certification.

SANS Institute
The SANS (System Administration, Networking, and Security) Institute was established in 1989 as a cooperative research and education organization. The SANS Institute enables more than 156,000 security professionals, auditors, system administrators, and network administrators to share the lessons they are learning and find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community. In 1999, SANS founded GIAC, which evolved into the Global Information Assurance Certification program. Funded solely by its own certification process, the GIAC program has been growing steadily ever since its creation and offers programs that address a range of skill sets, including security essentials, intrusion detection, incident handling, firewalls and perimeter protection, operating system security, and more. GIAC is unique in the field of information security certifications by not only testing a candidate's knowledge, but also testing a candidate's ability to put that knowledge into practice in the real world. Because of GIAC's practical focus, a Gartner Group study in the spring of 2001 named GIAC "the preferred credential" for individuals who have technical security responsibilities.

Table 2 shows various training methods and types used by companies that provide training programs to academic institutions.

BEST COPY AVAILABLE

Table 2. Training Methods and Types

Corporate Training Products									
Vendor	Instructor-led commercial training	Instructor-led college training	Self-study (CD-ROM)	Web-based training	Hard copy: lesson plans and lab books	Professional certifications	Instructor training	Remote course delivery	Vendor-neutral courses
3Com	X	X		X		3CSA, 3CSE			
Check Point	X					CCSA, CCSE, CCSE+, CCQE, CCAE			
Cisco	X	X	X	X	X	CCNA, CCNP, CCIP, CCAI, CCIE	X	X	X
ISS	X								X
Microsoft	X	X	X	X	X	MCP, MCSA, MCSE	X	X	X
NetScreen	X					NCSA, NCSP			
SonicWall	X					CSSA			
Sun	X	X	X	X	X	Java, SCSA, SCNA	X	X	X
Symantec	X					SCSP, SCSE, SPS			

BEST COPY AVAILABLE

Deciding on a Model

One of the first steps an academic institution should take to determine which model to use is to identify product trends and market share. Tables 3 and 4 illustrate the analysis of sample vertical markets within the IT security industry. An academic institution that wants to provide training should identify which technologies and products have the largest market share, then investigate what training programs, certification objectives, and academic partnerships the products' vendors offer.

Table 3. Five Popular Network Vulnerability Scanning Tools

Product	Vendor
Internet Scanner	Internet Security Systems
Nessus	Nessus
CyberCop Scanner	PGP Security/Network Associates
NetRecon	Symantec
Cisco Secure Scanner	Cisco

Table 4. Six Popular Intrusion Detection Systems

Product	Vendor
Shadow	Naval Surface Warfare Center
Snort!	Marty Roesch
Network Flight Recorder	NFR
RealSecure	Internet Security Systems (ISS)
Intrusion Detection System	Cisco
NetProwler	Symantec

BEST COPY AVAILABLE

Conclusion

A two-year institution that wants to establish an effective IT security program must take a diverse approach to curriculum adoption and development. The three main steps for developing effective skills-based training are

- Identify the local workforce needs
- Identify curriculum that can be adopted or used to provide a model for developing programs
- Identify and establish program benchmarks to measure program success

Academic programs should reflect the objectives of industry certifications. Obstacles to developing or adopting curricula are

- Vendors' limitations on the use of curriculum
- Instructor training and certification
- Equipment and software requirements
- The expense of partnership

Finally, organizations such as ISC, SANS, and CompTIA can provide academic institutions with invaluable direction in selecting products, curricula, technologies, and training materials.

White Paper

10. Trustworthy Computing

Craig Mundie, Microsoft Coporation
Pierre de Vries, Microsoft Corporation
Peter Haynes, Microsoft Corporation
Matt Corwine, Microsoft Corporation

The following paper was previously published by the Microsoft Corporation in May 2002. It is reprinted here with permission.

Why Trust?

While many technologies that make use of computing have proven themselves extremely reliable and trustworthy—computers helped transport people to the moon and back, they control critical aircraft systems for millions of flights every year, and they move trillions of dollars around the globe daily—they generally haven't reached the point where people are willing to entrust them with their lives, implicitly or explicitly. Many people are reluctant to entrust today's computer systems with their personal information, such as financial and medical records, because they are increasingly concerned about the security and reliability of these systems, which they view as posing significant societal risk. If computing is to become truly ubiquitous—and fulfill the immense promise of technology—we will have to make the computing ecosystem sufficiently *trustworthy* that people don't worry about its fallibility or unreliability the way they do today.

Trust is a broad concept, and making something trustworthy requires a social infrastructure as well as solid engineering. All systems fail from time to time; the legal and commercial practices within which they're embedded can compensate for the fact that no technology will ever be perfect.

Hence this is not only a struggle to make software trustworthy; since computers have to some extent already lost people's trust, we will have to overcome a legacy of machines that fail, software that fails, and systems that fail. We will have to persuade people that the systems, the software, the services, the people and the companies have all, collectively, achieved a new level of availability,

BEST COPY AVAILABLE

dependability and confidentiality. We will have to overcome the *distrust* that people now feel for computers.

The *Trustworthy computing initiative* is a label for a whole range of advances that have to be made for people to be as comfortable using devices powered by computers and software as they are today using a device that is powered by electricity. It may take us ten to 15 years to get there, both as an industry and as a society.

This is a "sea change" not only in the way we write and deliver software, but also in the way our society views computing generally. There are immediate problems to be solved, and fundamental open research questions. There are actions that individuals and companies can and should take, but there are also problems that can only be solved collectively by consortia, research communities, nations and the world as a whole.

Setting the Stage

History

Society has gone through a number of large technology shifts that have shaped the culture: the agrarian revolution, the invention of metalworking, the industrial revolution, the advent of electricity, telephony and television—and, of course, the microprocessor that made personal computing a reality. Each of these fundamentally transformed the way billions of people live, work, communicate and are entertained.

Personal computing has so far only really been deployed against white-collar work problems in the developed world. (Larger computer systems have also revolutionized manufacturing processes.) However, the steady improvement in technology and lowering of costs means that personal computing technology will ultimately become a building block of everybody's home and working lives, not just those of white-collar professionals.

Progress in computing in the last quarter century is akin to the first few decades of electric power. Electricity was first adopted in the 1880s by small, labor-intensive businesses that could leverage the technology's fractional nature to increase manufacturing productivity (i.e., a single power supply was able to power a variety of electric motors throughout a plant). In its infancy, electricity in the home was a costly luxury, used by high-income households largely for powering electric lights. There was also a good deal of uncertainty about the safety of electricity in general and appliances in particular. Electricity was associated with lightning, a lethal natural force, and there were no guarantees that sub-standard appliances wouldn't kill their owners.

Between 1900 and 1920 all that changed. Residents of cities and the fast-growing suburbs had increasing access to a range of energy technologies, and competition from gas and oil

pushed down electricity prices. A growing number of electric-powered, labor-saving devices, such as vacuum cleaners and refrigerators, meant that households were increasingly dependent on electricity. Marketing campaigns by electricity companies and the emergence of standards marks (e.g., Underwriters' Laboratories (UL) in the United States) allayed consumer fears. The technology was not wholly safe or reliable, but at some point in the first few years of the 20th century, it became safe and reliable *enough*.

In the computing space, we're not yet at that stage; we're still in the equivalent of electricity's 19th century industrial era. Computing has yet to touch and improve every facet of our lives—but it will. It is hard to predict in detail the eventual impact that computing will have, just as it was hard to anticipate the consequences of electricity, water, gas, telecommunications, air travel, or any other innovation. A key step in getting computing to the point where people would be as happy to have a microprocessor in every device as they are relying on electricity will be achieving the same degree of relative trustworthiness. "Relative," because 100% trustworthiness will never be achieved by any technology—electric power supplies surge and fail, water and gas pipes rupture, telephone lines drop, aircraft crash, and so on.

Trustworthy technologies in general

All broadly adopted technologies—like electricity, automobiles or phones—have become trusted parts of our daily lives because they are almost always there when we need them, do what we need them to do, work as advertised.

Almost anyone in the developed world can go buy a new telephone handset and plug it into the phone jack without worrying about whether it'll work or not. We simply assume that we'll get a dial tone when we pick up a phone, and that we'll be able to hear the other party when we connect. We assume that neither our neighbor nor the insurance broker down the road will be able to overhear our conversation, or obtain a record of who we've been calling. And we generally assume that the phone company will provide and charge for their service as promised. A combination of engineering, business practice, and regulation has resulted in people taking phone service for granted.

One can abstract three broad classes of expectations that users have of any trustworthy technology: safety, reliability and business integrity (i.e., the integrity of the organization offering the technology). These categories, and their implications for computing, are discussed in more detail below.

Trustworthy computing

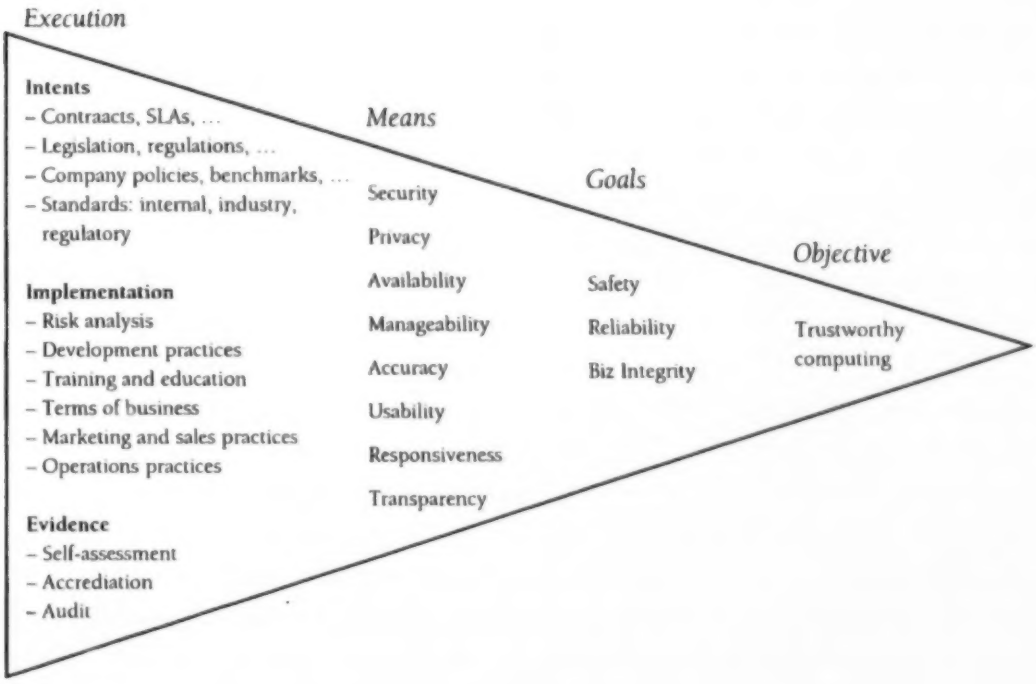
Computing devices and information services will only be truly pervasive when they are so dependable that we can just forget about them. In other words, at a time where computers are starting to find their way into just about every aspect of our life, we need to be able to trust them. Yet the way we build computers, and the way that we now build services around those computers, hasn't really changed that much in the last 30 or 40 years. It will need to.

A Framework for Trustworthy Computing

We failed to find an existing taxonomy that could provide a framework for discussing trustworthy computing. There is no shortage of trust initiatives, but the focus of each is narrow. For example, there are treatments of trust in e-commerce transactions and trust between authentication systems, and analyses of public perceptions of computing, but a truly effective approach needs to integrate engineering, policy and user attitudes. Even just on the engineering side, our scope is broader than, say, the SysTrust/SAS70 models, which deal purely with large online systems.

First, there are the machines themselves. They need to be reliable enough that we can embed them in all kinds of devices—in other words, they shouldn't fail more frequently than other similarly important technologies in our lives. Then there's the software that operates those machines: do people trust it to be equally reliable? And finally there are the service components, which are also largely software-dependent. This is a particularly complicated problem, because today we have to build dependability into an end-to-end, richly interconnected (and sometimes federated) system.

Since trust is a complex concept, it is helpful to analyze the objective of trustworthy computing from a number of different perspectives. We define three dimensions with which to describe different perspectives on trust: Goals, Means, and Execution.



Goals

The *Goals* consider trust from the user's point of view. The key questions are: Is the technology there when I need it? Does it keep my confidential information safe? Does it do what it's supposed to do? And do the people who own and operate the business that provides it always do the right thing? These are the goals that any trustworthy computing has to meet:

Goals	The basis for a customer's decision to trust a system
Safety	The customer's information and transactions are private and safe.
Reliability	The customer can depend on the product to fulfill its functions when required to do so.
Business Integrity	The vendor of a product behaves in a responsive and responsible manner.

The trust Goals cover both rational expectations of performance—i.e., those that are amenable to engineering and technology solutions—and more subjective assessments of behavior that are the result of reputation, prejudice, word of mouth, and personal experience. All of these goals raise issues relating to engineering, business practices and public perceptions, although not all to the same degree. In order to clarify terms, here are examples for the *Goals*:

- **Safety**: My personal information isn't disclosed in unauthorized ways. A virus doesn't infect and crash my PC. An intruder cannot render my system unusable or make unauthorized alterations to my data.
- **Reliability**: When I install new software, I don't have to worry about whether it will work properly with my existing applications. I can read my email whenever I want by clicking the Hotmail link on msn.com. I never get "system unavailable" messages. The Calendar doesn't suddenly lose all my appointments.
- **Business Integrity**: My service provider responds rapidly and effectively when I report a problem.

Means

Once the Goals are in place, we can look at the problem from the industry's point of view. *Means* are the business and engineering considerations that are employed to meet the Goals; they are the nuts and bolts of a trustworthy service. Whereas the Goals are largely oriented towards the end-user, the Means are inwardly facing, intra-company considerations. Think of the Goals as *what* is delivered, and the Means as *how*.

BEST COPY AVAILABLE

Means	The business and engineering considerations that enable a system supplier to deliver on the Goals
Security	Steps have been taken to protect the confidentiality, integrity and availability of data and systems.
Privacy	End-user data is never collected and shared with people or organizations without the consent of the individual. Privacy is respected when information is collected, stored and used consistent with Fair Information Practices.
Availability	The system is present and ready for use as required.
Manageability	The system is easy to install and manage, relative to its size and complexity. (Scalability, efficiency and cost-effectiveness are considered to be part of manageability.)
Accuracy	The system performs its functions correctly. Results of calculations are free from error, and data is protected from loss or corruption.
Usability	The software is easy to use and suitable to the user's needs.
Responsiveness	The company accepts responsibility for problems, and takes action to correct them. Help is provided to customers in planning for, installing and operating the product.
Transparency	The company is open in its dealings with customers. Its motives are clear, it keeps its word, and customers know where they stand in a transaction or interaction with the company.

Some examples:

- **Security**: An architecture might be designed to use triple-DES encryption for sensitive data such as passwords before storing them in a database, and the use of the SSL protocol to transport data across the Internet.
- **Privacy**: Technologies and standards such as P3P give users awareness and control of how their data is collected and used. At the same time, Microsoft has established clear privacy principles and set of policies that guide its behavior.
- **Availability**: The operating system is chosen to maximize MTBF (Mean Time Between Failures). Services have defined and communicated performance objectives, policies and standards for system availability.
- **Manageability**: The system is designed to be as self-managing as practicable. Hotfixes and software updates can be installed with minimal user intervention.
- **Accuracy**: The design of a system includes RAID arrays, sufficient redundancy and other means to reduce loss or corruption of data.
- **Usability**: The user interface is uncluttered and intuitive. Alerts and dialog boxes are helpful and appropriately worded.
- **Responsiveness**: Quality-assurance checks occur from early on in a project. Management makes it clear that reliability and security take precedence over feature richness or ship date. Services are constantly monitored and action is taken whenever performance doesn't meet stated objectives.
- **Transparency**: Contracts between businesses are framed as win-win arrangements, not an opportunity to extract the maximum possible revenue for one party in the short term. The company communicates clearly and honestly with all its stake holders.

BEST COPY AVAILABLE

Execution

Execution is the way an organization conducts its operations to deliver the components required for Trustworthy Computing. There are three aspects to this: Intents, Implementation and Evidence. *Intents* are the corporate and legislative guidance that sets requirements for the design, implementation and support of the product. *Implementation* is the business process that operationalizes the Intents. *Evidence* is the mechanism by which we verify that the Implementation has delivered on the Intent. Some examples:

Intents	• Company policies, directives, benchmarks, guidelines • Contracts and undertakings with customers, including Service Level Agreements (SLAs) • Corporate, industry and regulatory standards • Government legislation, policies and regulations.
Implementation	• Risk analysis • Development practices, including architecture, coding, documentation and testing • Training and education • Terms of business • Marketing and sales practices • Operations practices, including deployment, maintenance, sales and support, and risk management • Enforcement of intents and dispute resolution
Evidence	• Self-assessment • Accreditation by third parties • External audit

This problem can only be tackled by working on two parallel tracks.

The first track is the immediate problems—what people read and worry about every day. We need to address known current problems and mitigate currently known weaknesses. This is also a way to learn about the more fundamental problems. We need to be as well-informed as we can about what is really going on and what we can and cannot fix within the constraints of the current systems.

Part of the reason for customer anxiety is that personal computers are now entering areas that they didn't previously worry about. It will be easiest to focus on areas like banking or banking services where such problems are well known and of long standing.

While there is a lot of work to be done through incrementally improving current systems, these efforts will not solve the fundamental problems, some of which are described in the next section.

The computer industry needs to identify and solve the most critical challenges, and fold the solutions in an incremental way into the huge legacy systems that have been built. There

will be long technological replacement cycle during which the critical infrastructure systems that society depends on are gradually upgraded to a new and improved status. If these systems already exist, people are not just going to throw them out the window and start over from scratch. So we have to identify critical infrastructure and systems weaknesses and upgrade them on a high-priority basis, and ensure that new infrastructures are built on sound principles.

Fundamental Problems

Policy

Once a technology has become an integral part of how society operates, that society will be more involved in its evolution and management. This has happened in railways, telecommunications, TV, energy, etc. Society is only now coming to grips with the fact that it is critically dependent on computers.

We are entering an era of tension between the entrepreneurial energy that leads to innovation and society's need to regulate a critical resource despite the risk of stifling competition and inventiveness. This is exacerbated by the fact that social norms and their associated legal frameworks change more slowly than technologies. The computer industry must find the appropriate balance between the need for a regulatory regime and the impulses of an industry that has grown up unregulated and relying upon *de facto* standards.

Many contemporary infrastructure reliability problems are really policy issues. The state of California's recent electricity supply crisis was triggered largely by a bungled privatization. The poor coverage and service of US cellular service providers is due in part to the FCC's policy of not granting nationwide licenses. These policy questions often cross national borders, as illustrated by the struggle to establish global standards for third-generation cellular technologies. Existing users of spectrum (often the military) occupy different bands in different countries, and resist giving them up, making it difficult to find common spectrum worldwide.

Processing

Complexity

We are seeing the advent of mega-scale computing systems built out of loose affiliations of services, machines and application software. The emergent (and very different) behavior of such systems is a growing long-term risk.

An architecture built on diversity is robust, but it also operates on the edge of chaos. This holds true in all very-large-scale systems, from natural systems like the weather to human-

made systems like markets and the power grid. All the previous mega-scale systems that we've built—the power grid, the telephone systems—have experienced unpredicted emergent behavior. That is why in 1965 the power grid failed and rippled down the whole East Coast of the United States, and that's why whole cities occasionally drop off the telephone network when somebody implements a bug fix on a single switch. The complexity of the system has outstripped the ability of any one person—or any single entity—to understand all of the interactions.

Incredibly secure and trustworthy computer systems exist today, but they are largely independent, single-purpose systems that are meticulously engineered and then isolated. We really don't know what's going to happen as we dynamically stitch together billions—perhaps even trillions—of intelligent and interdependent devices that span many different types and generations of software and architectures.

As the power of computers increase, in both storage and computational capacity, the absolute scale and complexity of the attendant software goes up accordingly. This manifests itself in many ways, ranging from how you administer these machines to how you know when they are broken, how you repair them, and how you add more capability. All these aspects ultimately play into whether people perceive the system as trustworthy.

Hardware, Redundancy

We don't yet have really good economical, widely used mechanisms for building ultra-reliable hardware. However, we do have an environment where it may become common-place to have 200+ million transistors on a single chip. At some point it becomes worthwhile to make that into four parallel systems that are redundant and therefore more resistant to failure. The marginal cost of having this redundancy within a single component may be acceptable. Similarly, a computer manufacturer or end user may choose to install two smaller hard drives to mirror their data, greatly improving its integrity in the event of a disk crash.

We may have new architectural approaches to survivability in computer systems these days, but it always comes from redundancy. This means you have to buy that redundancy. So people will, in fact, again have to decide: Do they want to save money but potentially deal with more failure? Or are they willing to spend more money or deal with more complexity and administrative overhead in order to resolve the appropriate aspects of security, privacy, and technological sufficiency that will solve these problems?

Machine-to-Machine Processes

The Web Services model is characterized by computing at the edge of the network. Peer-to-peer applications will be the rule, and there will be distributed processing and storage. An administrative regime for such a system requires sophisticated machine-to-machine processes. Data will be self-describing. Machines will be loosely coupled, self-configuring, and self-organizing. They will manage themselves to conform to policy set at the center.

Web applications will have to be designed to operate in an asynchronous world. In the PC paradigm, a machine knows where its peripherals are; the associations have been established (by the user or by software) at some point in the past. When something disrupts that synchronicity, the software sometimes simply hangs or dies. Improved plug-and-play device support in Windows XP and "hot-pluggable" architectures such as USB and IEEE 1394 point the way toward a truly "asynchronous" PC, but these dependencies do still exist at times.

On the Web, however, devices come and go, and latency is highly variable. Robust Web architectures need dynamic discoverability and automatic configuration. If you accept the idea that everything is loosely coupled and asynchronous, you introduce even more opportunities for failure. For every potential interaction, you have to entertain the idea that it won't actually occur, because the Web is only a "best-effort" mechanism—if you click and get no result, you click again. Every computing system therefore has to be redesigned to recover from failed interactions.

Identity

Questions of identity are sometimes raised in the context of trustworthy computing. Identity is not explicitly called out in the framework, since a user does not expect a computer system to generate their identity. However, user identity is a core concept against which services are provided. Assertions of identity (i.e. authentication) need to be robust, so that taking actions that depend on identity (i.e. authorization) can be done reliably. Hence, users expect their identities to be safe from unwanted use.

Identity is difficult to define in general, but particularly so in the digital realm. We use the working definition that identity is the persistent, collective aspects of a set of distinguishing characteristics by which a person (or thing) is recognizable or known. Identity is diffuse and context-dependent since these aspect "snippets" are stored all over the place in digital, physical and emotional form. Some of this identity is "owned" by the user, but a lot of it is conferred by others, either legally (e.g., by governments or companies) or as informal social recognition.

Many elements of trustworthy computing systems impinge on identity. Users worry about the privacy of computer systems in part because they realize that seemingly unrelated aspects of their identity can be reassembled more easily when the snippets are in digital form. This is best evidenced by growing public fear of credit-card fraud and identity theft as a result of the relative transparency and anonymity of the Internet vs. offline transactions, even though both crimes are equally possible in the physical world. Users expect that information about themselves, including those aspects that make up identity, are not disclosed in unapproved ways.

People

It's already challenging to manage extremely large networks of computers, and it's just getting harder. The immensity of this challenge has been masked by the fact that up to this point we have generally hired professionals to manage large systems. The shortcomings of the machines, the networks, the administration, the tools, and the applications themselves are often mitigated by talented systems managers working hard to compensate for the fact that these components don't always work as expected or desired.

Many of the system failures that get a lot of attention happen because of system complexity. People make an administrator error, fail to install a patch, or configure a firewall incorrectly, and a simple failure cascades into a catastrophic one. There is a very strong dependency on human operators doing the right thing, day in and day out.

There are already too few knowledgeable administrators, and we're losing ground. Worse, the needs of administration are evolving beyond professional IT managers. On the one hand we are at the point where even the best operators struggle: systems are changing too rapidly for people to comprehend. On the other, the bulk of computers will eventually end up in non-managed environments that people own, carry around with them, or have in their car or their house.

We therefore need to make it easier for people to get the right thing to happen consistently with minimal human intervention. We must aim towards a point where decision-makers can set policy and have it deployed to thousands of machines without significant ongoing effort in writing programs, pulling levers and pushing buttons on administrators' consoles.

The industry can address this in any of a number of ways. Should we actually write software in a completely different way? Should we have system administrators at all? Or should we be developing machines that are able to administer other machines without routine human intervention?

Programming

Tools

Each of these approaches requires new classes of software. As the absolute number and complexity of machines goes up, the administration problem outstrips the availability and capability of trained people.

The result is that people in the programming-tools community are going to have to think about developing better ways to write programs. People who historically think about how to manage computers are going to have to think about how computers can become more self-organizing and self-managing.

We need to continue to improve programming tools, since programming today is too error-prone. But current tools don't adequately support the process because of the number of abstraction layers that require foreground management. In other words, the designer needs not only to consider system architecture and platform/library issues, but also everything from performance, localization and maintainability to data structures, multithreading and memory management. There is little support for programming in parallel, most control structures are built sequentially and the entire process is painfully sequential. And that is just in development; at the deployment level it is incredibly difficult to test for complex interactions of systems, versions, and the huge range in deployment environments. There is also the increasing diffusion of tools that offer advanced development functionality to a wider population but do not help novice or naive users write good code. There are also issues around long-term perspectives: for example, tools don't support "sunset-ing" or changing trends in capability, storage, speed, and so on. Think of the enormous effort devoted to Y2K because programmers of the 1960s and 1970s did not expect their code would still be in use on machines that far outstripped the capabilities of the machines of that era.

Interoperability

The growth of the Internet was proof that interoperable technologies—from TCP/IP to HTTP—are critical to building large-scale, multipurpose computing systems that people find useful and compelling. (Similarly, interoperable standards, enforced by technology, policy or both, have driven the success of many other technologies, from railroads to television.) It is obvious and unavoidable that interoperable systems will drive computing for quite some time.

But interoperability presents a unique set of problems for the industry, in terms of technologies, policies and business practices. Current "trustworthy" computing systems, such as the air-traffic-control network, are very complex and richly interdependent, but they are also engineered for a specific purpose, rarely modified, and strictly controlled by a central authority. The question remains whether a distributed, loosely organized, flexible and dynamic computing system—dependent on interoperable technologies—can ever reach the same level of reliability and trustworthiness.

Interoperability also poses a problem in terms of accountability and trust, in that responsibility for shortcomings is more difficult to assign. If today's Internet—built on the principle of decentralization and collective management—were to suffer some kind of massive failure, who is held responsible? One major reason why people are reluctant to trust the Internet is that they can't easily identify who is responsible for its shortcomings—who would you blame for a catastrophic network outage, or the collapse of the Domain Name System? If we are to create and benefit from a massively interoperable (and interdependent) system that people can trust, we must clearly draw the lines as to who is accountable for what.

Conceptual models

We face a fundamental problem with trustworthy computing: computer science lacks a theoretical framework. Computer security—itself just one component of trustworthy computing—has largely been treated as an offshoot of communications security, which is based on cryptography. Cryptography has a solid mathematical basis, but is clearly inadequate for addressing the problems of trusted systems. As Microsoft researcher Jim Kajiya has put it, "It's as if we're building steam engines but we don't understand thermodynamics." The computer-science community has not yet identified an alternative paradigm; we're stuck with crypto. There may be research in computational combinatorics, or a different kind of information theory that seeks to study the basic nature of information transfer, or research in cooperative phenomena in computing, that may eventually form part of an alternative. But, today this is only speculation.

A computing system is only as trustworthy as its weakest link. The weakest link is all too frequently human: a person producing a poor design in the face of complexity, an administrator incorrectly configuring a system, a business person choosing to deliver features over reliability, or a support technician falling victim to impostors via a "social engineering" hack. The interaction between sociology and technology will be a critical research area for trustworthy computing. So far there is hardly any cross-fertilization between these fields.

Summary

- Delivering trustworthy computing is essential not only to the health of the computer industry, but also to our economy and society at large.
- Trustworthy computing is a multi-dimensional set of issues. All of them accrue to three goals: safety, reliability and business integrity. Each demands attention.
- While important short-term work needs to be done, hard problems that require fundamental research and advances in engineering will remain.
- Both hardware and software companies, as well as academic and government research institutions, need to step up to the challenge of tackling these problems.

Appendix

Workshop Agenda

The Role of Community Colleges in Cybersecurity Education

A Workshop Sponsored by
The National Science Foundation and
The American Association of Community Colleges

Renaissance Mayflower Hotel, Washington, D.C., June 26–28, 2002

Agenda

Wednesday, June 26, 2002		
4:00–8:00 p.m. *Outside of East Room*	**Workshop Registration**	
6:00 p.m. *East Room*	**Welcome** *Elizabeth Teles*, Lead Program Director, Advanced Technological Education, National Science Foundation *Kristen Duerr*, Senior Vice President and Publisher, Thomson-Course Technology	
6:15 p.m.	**Remarks and Introduction of Speaker** *Joe Bordogna*, Deputy Director, National Science Foundation	
6:30 p.m.	**Opening Keynote Address** *Howard Schmidt*, Vice Chair, President's Critical Infrastructure Protection Board	
7:15 p.m. *East Room*	**Dinner** Sponsored by Thomson–Course Technology	
8:15 p.m. *East Room*	**Session 1: Trustworthy Computing** **Introduction of Speaker** *Neil Evans*, Executive Director, National Workforce Center for Emerging Technologies **Keynote Address** *Craig Mundie*, Senior Vice President and Chief Technical Officer, Advanced Strategies and Policy, Microsoft Corporation	**Background Reading:** Craig Mundie et al., "Trustworthy Computing"
9:00 p.m.	**Q & A with Craig Mundie** Moderator: *Neil Evans*	
9:45 p.m.	**Adjourn**	

BEST COPY AVAILABLE

Thursday, June 27, 2002		
7:30 am–noon *Outside of East Room*	**Workshop Registration**	
7:30 a.m. *East Room*	**Continental Breakfast** Participants who reserved display tables can set out brochures or materials at this time. The breakfast is a non-structured event. Participants may come at their leisure between 7:30–8:30 a.m.	
8:30 a.m. *East Room*	**Session 2: Cybercrime** Moderator: *Thomas Akin*, Southeast Cybercrime Institute Presenters: *Fred Cotton*, SEARCH, Inc. *Dave Curran*, N.Y. Electronic Crimes Task Force, U.S. Secret Service *John Frazzini*, Electronic Crimes Branch, U.S. Secret Service *Raemarie Schmidt*, National White Collar Crime Center	**Background Reading:** Richard Power, "2002 CSI/FBI Computer Crime and Security" (*Computer Security Issues and Trends* vol. 8, no. 1 [Spring 2002])
9:30 a.m. *East Room*	**Session 3: Foundations for Cybersecurity Curricula** Moderator: *Peter Saflund*, National Workforce Center for Emerging Technologies Presenters: *Kris Madura*, CompTIA *Corey Schou*, Idaho State University	**Background Reading:** Neil Evans et al., "IT Security Specialist: Integrating Academic Credentials with IT Professional Certifications"
10:30 a.m. *East Room and upstairs breakout rooms*	**Refreshment Break**	
10:45 a.m. *Upstairs breakout rooms*	**Breakout Group Meetings** Group A–East Room Group B–Pennsylvania Room Group C–Rhode Island Room Group D–South Carolina Room Group E–Virginia Room	
11:45 a.m. *East Room*	**Report-Back from Breakout Groups**	
12:15 p.m. *East Room*	**Lunch** **Remarks:** *George Boggs*, President and CEO, American Association of Community Colleges *Judith Ramaley*, Assistant Director for Education and Human Resources, National Science Foundation	
1:15 p.m.	**Break**	

BEST COPY AVAILABLE

Thursday, June 27, 2002 (continues)		
1:30 p.m. *East Room*	**Session 4: Cybersecurity Literacy** Moderator: *Corby Hovis*, National Science Foundation Presenters: *Kirk Bailey*, University of Washington and City of Seattle *Jim Litchko*, Lichko and Associates *Randy Marchany*, Virginia Tech	
2:30 p.m. *East Room*	**Session 5: Current Cybersecurity Courses and Curricula** Moderator: *Robert Campbell*, Rock Valley College Presenters: *Matthias Giessler*, Cisco Systems *Keith Morneau*, Northern Virginia Community College *Gregory White*, University of Texas, San Antonio	**Background Reading:** Robert D. Campbell and Elizabeth K. Hawthorne, "Cybersecurity Education in Community Colleges Across America: A Survey of Four Approaches by Five Institutions" Erich Spengler and Aurora Zwick, "Adapting Commercial Training Materials for Use at the Community College"
3:30 p.m. *East Room and upstairs breakout rooms*	**Refreshment Break**	
3:45 p.m. *Upstairs breakout rooms*	**Breakout Group Meetings** Group A–East Room Group B–Pennsylvania Room Group C–Rhode Island Room Group D–South Carolina Room Group E–Virginia Room	
4:45 p.m. *East Room*	**Report-Back from Breakout Groups**	
5:15 p.m. *East Room*	**Session 6: Hiring Cybersecurity Professionals** Moderator: *Shirley Malia*, Cybersecurity Workforce Consultant Presenters: *George Bieber*, Defense-Wide Information Assurance Program, U.S. Dept. of Defense *Jim Brenton*, Sprint Corporate Security *James Joyce*, TechGuard Security	
6:15 p.m. *East Room*	**Reception** Visit display tables	
7:00 p.m.	**Adjourn** There will be dinner groups going to area restaurants. Sign-up sheets for dinner groups will be posted in the East Room.	

BEST COPY AVAILABLE

Friday, June 28, 2002		
7:30 a.m. *East Room*	**Continental Breakfast** The breakfast is a non-structured event. Participants may come at their leisure between 7:30–8:30 a.m.	
8:30 a.m. *East Room*	**Introduction of Speaker** *Norman Fortenberry*, Director, Division of Undergraduate Education, National Science Foundation **Keynote Address** *William A. Wulf*, President, National Academy of Engineering, and AT&T Professor of Engineering and Applied Science, University of Virginia	
9:30 a.m. *East Room*	**Session 7: Establishing and Maintaining a Cybersecurity Program** Moderator: *Marie Wright*, Western Connecticut State University Presenters: *Julie Ryan*, George Washington University *Sujeet Shenoi*, University of Tulsa *Craig Tidwell*, Seminole Community College	**Background Reading:** Barbara Belon and Marie Wright, "Case Study: Creation of a Degree Program in Computer Security"
10:30 a.m. *East Room and upstairs breakout rooms*	**Refreshment Break**	
10:45 a.m. *Upstairs breakout rooms*	**Breakout Group Meetings** Group A–East Room Group B–Pennsylvania Room Group C–Rhode Island Room Group D–South Carolina Room Group E–Virginia Room	
12:00 p.m. *East Room*	**Report-Back from Breakout Groups and Wrap-Up of Workshop**	
12:30 p.m.	**Adjourn**	

Reports from the workshop sessions, including responses from each breakout group, can be found on the Web at www.aacc.nche.edu/cybersecurity

BEST COPY AVAILABLE

Appendix

Keynote Speaker Biographies

Craig Mundie

Craig Mundie is the chief technical officer of advanced strategies and policy for Microsoft Corporation, where he reports to chairman and chief software architect Bill Gates and works with him on developing a comprehensive set of technical, business, and policy strategies. As part of his current role, Mundie is involved in policy-related activities encompassing security, privacy, encryption, and telecom regulation. He works with government and business leaders in Washington, D.C., to address these issues. In August 2000 President Clinton named Mundie to the National Security Telecommunications Advisory Committee, which was created in 1982 to advise the White House on issues affecting the security of the nation's telecommunications infrastructure. In February 2002 Mundie became a member of the Council on Foreign Relations, a nonpartisan membership organization, research center, and publisher dedicated to increasing America's understanding of the world and contributing ideas to U.S. foreign policy. In April 2002 he became a member of the Task Force on National Security in the Information Age, whose main project is to develop a strategy for using new technologies and information to address new security challenges.

Howard A. Schmidt

Howard A. Schmidt was appointed by President George W. Bush as a special assistant to the president and the vice chair of the President's Critical Infrastructure Protection Board in December 2001. The board focuses on building a specialized group of senior government and private sector leaders to focus on cybersecurity issues and security-related incidents. Schmidt is also a distinguished special lecturer at the University of New Haven, Connecticut, teaching a graduate certificate course in forensic computing.

William A. Wulf

William A. Wulf is on leave from the University of Virginia to serve as president of the National Academy of Engineering (NAE). Together with the National

120 BEST COPY AVAILABLE

Academy of Sciences, the NAE operates under a congressional charter to provide advice to the government on issues of science and technology. Much of this advice is provided through the National Research Council (NRC), the operating arm of the two academies; Wulf serves as vice chair of the NRC.

At the University of Virginia, Wulf is a professor and holds the AT&T Chair in Engineering and Applied Science. His activities include completely revising the undergraduate computer science curriculum, researching computer architecture and computer security, and assisting humanities scholars in exploiting information technology.

Appendix

Cybersecurity Education Resources

1. National Science Foundation Program Web sites

www.nsf.gov National Science Foundation Main Page
www.ehr.nsf.gov/due/programs/ate/ Advanced Technological Education Program (ATE)
www.ehr.nsf.gov/due/programs/sfs/ Federal Cyber Service: Scholarship for Service (SFS)

2. Acronyms and Glossary of Cybersecurity Certifications

ASIS: American Society for Industrial Security (see CPP).

CCSP (Cisco Certified Security Professional). Cisco offers two security certifications at present: CCIE Security and Cisco Security Specialist 1. **www.cisco.com/warp/public/625/ccie/certifications/security.html** and **www.cisco.com/warp/public/10/wwtraining/certprog/pdf/css1.pdf**.

CFE (Computer Fraud Examiner): Certification administered by the Association of Certified Fraud Examiners—**http://marketplace.cfenet.com/membership/uniformcfeexamination.asp**.

CISA (Certified Information Systems Auditor): Certification administered by the Information Systems Audit and Control Association (ISACA)—**www.isaca.org/cert1.htm**.

CISSP: Certified Information Systems Security Professional, a certification administered by $(ISC)^2$—**www.isc2.org/cgi-bin/content.cgi?category=19**.

CNSS 4011, 4012, 4012, 4014, 4015: The major national training standards for information security professionals (NSTISSI), which serve as the foundation for NSA-approved university curricula in information security. The following were developed as the NSTISSI standards:

NSTISSI 4011—National Training Standard for Information Systems Security (INFOSEC) Professionals

BEST COPY AVAILABLE

NSTISSI 4012—National Training Standard for Designated Approving Authority (DAA)
NSTISSI 4013—National Training Standard for System Administration in Information Systems Security
NSTISSI 4014—National Training Standard for Information Systems Security Officers (ISSO)
NSTISSI 4015—National Training Standard for Systems Certifiers

CNSS is the new designation. See the links to the detailed standards documents at **www.nstissc.gov/html/library.html**

CPP: Certified Protection Professional, the certification administered by ASIS—**www.asisonline.org/cppg/cpphome.html**.

DRI: The Disaster Recovery Institute (DRI) offers three certifications—**www.drii.org/certification.html**

GIAC (Global Information Assurance Certification): **www.giac.org**.

MSP (Microsoft Security Professional): Microsoft certifications—**www.microsoft.com/traincert/mcp/default.asp**.

Security+: CompTIA's new security certification—**www.comptia.org/certification/securityplus/index.htm**.

3. Information Security Related–Online Publications and Web Sites

K–12 Education
www.staysafeonline.com Kid-friendly guide to the Internet

Higher Education
www.aacc.edu/cybercrime Anne Arundel Community College's Cybercrime Studies Institute
http://apec.isu.edu APEC Academic Program
www.csa.syr.edu/education.htm Center for Systems Assurance
www.cerias.purdue.edu/coast/ COAST at Purdue University
http://csrc.lse.ac.uk Computer Security Research Center, London School of Economics
www.au.af.mil/au/ccaf/catalog/2002cat/ter_0iyy.htm Community College of the Air Force
www.emse.gwu.edu/emse/program/masters/ism.html Engineering Management and Systems Engineering at GWU
http://security.isu.edu Idaho State University Information Security Resources
www.iup.edu/infosecurity Information Assurance Education at Indiana University of Pennsylvania
www.cs.fsu.edu/infosec/ Information Technology Assurance and Security at Florida State University
www.ists.dartmouth.edu/ Institute for Security Technology Studies, Dartmouth College
http://cisse.info National Colloquium for Information Systems Security Education

www.nsa.gov/isso/programs/nietp/newspg1.htm NSA's National INFOSEC Education and Training Program
www.nvcc.vccs.edu/curcatalog/descript/ist248.htm Northern Virginia Community College
www.jmu.edu/computing/runsafe/ RUNSAFE, James Madison University
www.sait.fsu.edu SAIT Security and Assurance in Information Technology Laboratory at Florida State University
www.scc-fl.edu/e-business/securityasdegreecourses.htm Seminole Community College
www.seas.gwu.edu/~infosec/ Studying Information Assurance and Security at GWU
http://seclab.cs.ucdavis.edu/ University of California, Davis, Computer Security Laboratory
www.utsa.edu/cias University of Texas San Antonio Center for Infrastructure Assurance
www.wcsu.edu/asb/mis/ism.asp Western Connecticut State University

Corporate Education
www.cert.org/nav/index_gold.html Carnegie Mellon CERT Training and Education
www.checkpoint.com/services/education/aapprogram/index.html Check Point Education Services
www.comptia.org/certification/securityplus/index.htm CompTIA Security+ Certification
www.gocsi.com Computer Security Institute (CSI), The
www.itaa.org/infosec/awareness.htm Information Technology Association of America, Cybercitizen Partnership Awareness Campaign
www.staysafeonline.info/ Stay Safe Online
www.networkintrusion.co.uk Security Training Courses
www.securitycertified.net/certifications.htm Security Certified Program, by Ascendant Learning
www.course.com/security Thomson Course Technology

Home User/Small Office User
www.cert.org/tech_tips/home_networks.html Carnegie Mellon CERT Home Network Security
www.cisco.com/warp/public/778/security/vuln_stats_02-03-00.html Cisco Vulnerability Statistics Report
www.consumer.gov/idtheft Federal Trade Commission information about identity theft
www.tinysoftware.com/home/tiny2?la=EN Tiny Firewall for home

Homeland Security
www.fbi.gov/hq/nsd/ansir/ansir.htm Awareness of National Security Issues and Response (ANSIR) Program, FBI's National Security Awareness Program
www.ccc.nps.navy.mil/rsepResources/homeland.asp Department of National Security Affairs, Center for Contemporary Conflict

Government Sector
http://ciac.llnl.gov/cstc *CIAC's Cyber Solutions Tools Center(CSTC)*, at the Lawrence Livermore National Laboratory
http://csrc.nist.gov/csspab/ Computer System Security and Privacy Advisory Board

http://fedcirc.gov Federal Computer Incident Response Capability
http://csrc.nist.gov/organizations/fissea Federal Information Systems Security Educators' Association
www.istpa.org International Security Trust and Privacy Association
http://csrc.nist.gov/fasp/ NIST Federal Agency Security Practices
www.orau.gov/se/ Security Education Special Interest Group, The
www.twurled-world.com/SecTraining/cover.htm U.S. Government Security Expertise

Government
http://chacs.nrl.navy.mil Center for High Assurance Computing Systems, The
www.disa.mil Defense Information Systems Agency (Department of Defense)
www.fedcirc.gov/ Federal Computer Incident Response Center (FedCIRC), The
http://iase.disa.mil/ Information Assurance Support Environment
www.iatf.net/ Information Assurance Tech Framework Forum Education Links
www.nipc.gov/ National Infrastructure Protection Center
http://csrc.nist.gov NIST (National Institute of Standards and Technology)
wwwoirm.nih.gov/ Office of the Deputy Chief Information Officer
www.fts.gsa.gov/infosec/ Office of Information Security (OIS), The
www.nsa.gov/isso/index.html NSA INFOSEC
www.ncisse.org/Courseware/NSAcourses/ NSA Online Information Assurance Courses
http://doe-is.llnl.gov United States Department of Energy
www.usaid.gov/pubs/ads/500/security.html U.S. Aid Security Services
http://doe-is.llnl.gov/DOESecurityResources.html U.S. Department of Energy
www.ectaskforce.org U.S. Secret Service Electronic Crimes Task Force

General Security Sites
www.antionline.com/index.php AntiOnline.com
www.cerias.purdue.edu/ CERIAS / Purdue University
www3.ca.com/Solutions/Solution.asp?ID=271 Computer Associates Security
www.alw.nih.gov/Security/security.html Computer security information
www.isc2.com E-Fortress
www.prognosisx.com/infosyssec/index.html INFOSYSSEC, The Security Portal for Information System Security Professionals
http://interpactinc.com/sat.html Interpact Security Awareness Training
www.intrusion.com Intrusion.com Inc.
http://janusassociates.com/default.html Janus Associates, Inc.
www.trusecure.com Managed Security Services by TruSecure
http://csrc.nist.gov/ATE/ NSIT CSRS Awareness, Training and Education
http://security.sdsc.edu/ San Diego Supercomputer Center
www.sans.org/newlook/home.php SANS (SysAdmin, Audit, Network, Security) Institute
www.searchsecurity.com Search Security
www.securityawareness.com/ Security Awareness, Inc.
www.securityfocus.com Security Focus
www.securitynews.org/sources/edu.html Security News

www.securitywatch.com/EDU/fr_education.html Security Watch
http://enterprisesecurity.symantec.com/Default.cfm?PID=13041863&EID=261 Symantec Security Newsletter
www.techguardsecurity.com/education.html TechGuard Security®
www.whitehats.com Whitehats Network Security Resource

Security Certification
www.cccure.org/ CISSP Open Study Guides Web site
www.cisspworld.com/ CISSPworld project services the needs of CISSP certified professionals
www.isaca.org/isacafx.htm Information Systems Audit and Control Association®
www.isc2.org International Information Systems Security Certifications Consortium, Inc.
www.giac.org SANS Global Information Assurance Certification
http://securitycertified.net Security Certified Network Professional or Security Certified Network Architect
www.staysafeonline.info/enroll.adp Stay Safe Online, awareness of computer security–related issues
www.sscps.com/ Systems Security Certified Practitioner Portal

Security Periodicals
www.cisomagazine.com/ CISO Magazine
www.counterpane.com Counterpane Newsletter (Cryptogram)
https://wow.mfi.com/csi/order/frontline.html CSI FrontLine End-User Awareness Newsletter
www.csoonline.com CSO Magazine
www.infosecuritymag.com Information Security magazine, TruSecure
www.issa.org ISSA Password
www.itpapers.com/resources/tech_guides.html IT White Papers
www.itworld.com/Comp/2378/UnixInsider/ ITworld.com's collection of Unix news and information
www.itworld.com IT World, IT News, Webcast, White Papers, Newsletters
www.scmagazine.com/ Security Computing Magazine
www.securitymanagement.com/ Security Management Online
www.w2knews.com Sunbelt W2Knews Electronic Newsletter

Security Groups (other than ISSA)
www.gocsi.com Computer Security Institute
www.htcia.org/ High Tech Crime Investigation Association
www.infragard.net/ Infragard
www.misti.com MIS Training Institute
www.nw3c.org/ National White Collar Crime Center
www.training.nw3c.org National White Collar Crime Center
www.cybercrime.org National White Collar Crime Center, computer crime section
www.rsasecurity.com RSA Security

Microsoft Security and Best Practices

www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/default.asp Security Best Practices

www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/default.asp Security—Products and Technologies

www.houseofhelp.com/articles/win2k_guide/index.php Windows 2000 Security

Evidence Collection

www.porcupine.org/forensics/ Computer Forensic Analysis

www.cybercrime.gov/ Department of Justice, Computer Crime and Intellectual Property Section

www.digitalintel.com/ Digital Intelligence, Inc.

www.fbi.gov/hq/lab/fsc/current/index.htm FBI Forensic Science Communications

www.cops.org/forensic_examination_procedures.htm IACIS Computer Forensics Procedures

www.iwar.org.uk IWS—The Information Warfare Site

www.AllLaw.com/ Legal Resources

www.forensics-intl.com/evidguid.html New Technologies, Inc. Computer Evidence Processing Steps

www.forensics-intl.com/tools.html NTI's Forensic and Security Suites

www.cybercrime.gov/searchmanual.htm Searching and Seizing Computer and Obtaining Electronic Evidence in Criminal Investigations

Disaster Recovery

www.survive.com/ Business Continuity Group

www.rothstein.com/ Business Recovery Consulting and Educational Resources on Disaster Recovery

www.drj.com/ Disaster Recovery Journal

Articles

www.cl.cam.ac.uk/Research/Security/studies/st-proto.html Computer Security Group, University of Cambridge

http://esecurityonline.com/articles.asp esecurity portal has content in security news, events, tools, white papers, and editorials

www.educause.edu/asp/doclib/abstract.asp?ID=NET0027 Higher Education Contribution to National Strategy to Secure Cyberspace

http://www2.norwich.edu/mkabay/overviews/infosec_ed.htm Information Security Education Resources for Professional Development, Version 4—September 2001, M. E. Kabay, PhD, CISSP

www.robertgraham.com/ Infosec documents.

www.linuxsecurity.com/feature_stories/feature_story-8.html Intrusion Detection Primer, Linuxsecurity.com

www.trust-factory.com/falling-dominos.html Lotus Notes and Domino Security from Trust Factory

www.fish.com/security/murphy.html Murphy's law and computer security

www.secinf.net/ipolicye.html Network Security Information: Security Policy
www.washington.edu/R870/ Unix System Administration—A Survival Course O'Reilly and Associates: Computer Security Basics
www.nwfusion.com/newletters/careers/2002/01407540.html—What Work Requires of Schools: A SCANS Report for American 2000

Sun Security Configuration Document
www.sun.com/solutions/blueprints/0100/security.pdf

Tools
www.ealaddin.com Aladdin Knowledge Systems
www.sanctuminc.com AppShield by Sanctum Inc.
www.atstake.com/index.html @Stake, Inc. Digital Security
http://blackice.iss.net BlackICE™ protection
http://security.cw.net/ Cable and Wireless Security Alerts
www.checkpoint.com Check Point Software Technologies Ltd
www.clicknet.com ClickNet Security Technologies Corp.
www.cybersafe.com CyberSafe Corp.
www.cylant.com/index.php Cylant Technology, CylantSecure
www.eeye.com/html/index.html eEye Digital Security
www.enterasys.com/home.html Enterasys Networks Inc.
www.f-secure.com/ F-Secure, Securing the Mobile Enterprise
www.iss.net Internet Security Systems Inc.
www.intrusion.com Intrusion.com Inc.
www.research.att.com/sw/tools/ Learn about or acquire software tools developed at AT&T Labs Research
www.nessus.org Nessus Scanner
www.network-1.com/website Network-1 Security Solutions
www.olympussecurity.com Olympus Security Group
www.packetfactory.net/ Packetfactory is a clearinghouse for network security
www.pgp.com PGP Security (a Network Associates Inc. business)
www.ideahamster.org/ Penetration Testing Methodology
http://razor.bindview.com/tools/ Razor Bindview tools
www.silentrunner.com SilentRunner from Raytheon Co.
www.sourcefire.com Sourcefire, Inc.
www.tripwire.com TripWire Inc.
wwwinfo.cern.ch/dis/security/general/tools/toc.html Tools
www.wiretrip.net Whisker Application Scanner

Appendix

Workshop Participants

Frederick Ahrens
Curriculum Developer, Consultant
Clover Park Technical College
4500 Steilacoom Boulevard, SW
Lakewood, WA 98499-4098

Thomas Akin
Director
Southeast Cybercrime Institute
1000 Chastain Road, #3301
KSU Center Building #33
Kennesaw, GA 30144

Kirk Bailey
Manager
Strategic Computer Services
University of Washington
Computing and Communications
Mary Gates Hall, Suite 011
Box 352830
Seattle, WA 98195-2830

Matthew Basham
Program Director
Cisco Regional Networking Academy
St. Petersburg College
7887 Bryan Dairy Road
Largo, FL 33777

Barbara Belon
Director
Center for Information Technology
Norwalk Community College
188 Richards Avenue, 606D
Norwalk, CT 06854-1655

George Bieber
Chief
Information Assurance Human
Resources and Training Oversight
Defense-Wide Information Assurance
Program (DIAP)
U.S. Department of Defense
1215 Jefferson Davis Highway
Suite 1101
Arlington, VA 22202

Sherry Borror
Information Systems Security Analyst
National Security Agency
9800 Savage Road, Suite 6752
Ft. Meade, MD 20755

James Brenton
Principal Network Security Architect
Sprint Corporate Security
6480 Sprint Parkway
KSOPHM0206-2B376
Overland Park, KS 66251

Joan Calvert
Professor and Chair
Department of Computer Science
Central Connecticut State University
1615 Stanley Street
New Britain, CT 06455

***Robert Campbell**
CIO and Executive
Dean of Information
Rock Valley College
3301 N. Mulford Road
Rockford, IL 61114

BEST COPY AVAILABLE

129

Alice Cohen
Chair
Department of Computer Information Systems
Borough of Manhattan Community College
199 Chambers Street
New York, NY 10019

Fred Cotton
Director of Training Services
SEARCH, Inc.
7311 Greenhaven Drive, Suite 145
Sacramento, CA 95831

Seth Cox
Principal/Executive Vice President
iSecurePrivacy, Inc.
13811 Pearl Lane
Moreno Valley, CA 92555

David Croghan
Dean
Workforce Development and Business Services
Anne Arundel Community College
101 Crain Highway, NE
Glen Burnie, MD 21061

David Curran
Deputy Director
New York Electronic Crimes Task Force
U.S. Secret Service
335 Adams Street, 32nd Floor
Brooklyn, NY 11201

Vanessa Dedeaux
Instructor
Web Development Program
Mississippi Gulf Coast Community College
PO Box 548
Perkinston, MS 39573

Kristen Duerr
Senior Vice President and Publisher
Thomson-Course Technology
25 Thomson Place
Boston, MA 02210

Heather Dussault
Assistant Professor of Computer Science
SUNY Institute of Technology at Utica/Rome
School of Information Systems and Engineering Technology
Kunsela Hall, PO Box 3050
Utica, NY 13504-3050

Steve Elliot
Associate Publisher
Thomson-Course Technology
25 Thomson Place
Boston, MA 02210

John Engman
Director
Jobs+IT Workforce Development
National Workforce Center for Emerging Technologies/CompTIA
1815 S. Meyers Road
Oakbrook Terrance, IL 60181

Michael Erbschloe
Vice President
Research Computer Economics
5841 Edison Place, Suite 130
Carlsbad, CA 92008

***Neil Evans**
Executive Director
National Workforce Center for Emerging Technologies
Bellevue Community College
3000 Landerholm Circle, SE
N-258
Bellevue, WA 98007-6484

130

Patricia Fisher
President
JANUS Associates
1010 Summer Street
Stamford, CT 06905

John Frazzini
Special Agent
Electronic Crimes Branch
U.S. Secret Service
1100 L Street, NW
Washington, DC 20003

Mike Gadzus
U.S. Secret Service
Carnegie Mellon University

Henry Gee
Professor of Computer and Information Technology
Evergreen Valley College
3095 Yerba Buena Road
San Jose, CA 95135

Forouzan Golshani
Professor of Computer Science and Engineering
Arizona State University
Department of Computer Science and Engineering
Mail Stop 5406
Tempe, AZ 85287-5406

Russ Griffith
U.S. Secret Service
Carnegie Mellon University

Steve Hailey
Technical Trainer
Edmonds Community College
Business and Technology Center
728 134th Street SW, STE 128
Everett, WA 98204

Sheryl Hale
State Coordinator
Adult and Career Development Division
Oklahoma Department of Career and Technology Education
1500 W. 7th Avenue
Stillwater, OK 74074

Dennis Hansen
Instructor of Information Systems
Southeastern Community College
PO Box 151
Whiteville, NC 28472

***Elizabeth Hawthorne**
Assistant Professor of Computer Science
Union County College
1033 Springfield Avenue
Cranford, NJ 07016

Zoe Irvin
Executive Director
Planning, Research and Organizational Development
Howard Community College
10901 Little Patuxent Parkway
Columbia, MD 21044

Thomas Johnson
Dean
School of Public Safety and Professional Studies
University of New Haven
300 Orange Avenue
West Haven, CT 06516

Diane Jones
Professional Staff
Committee on Science, Subcommittee on Research
U.S. House of Representatives
Committee on Science
B-374 Rayburn House Office Building
Washington, DC 20515

131

James Joyce
Chief Technology Officer
TechGuard Security
743 Spirit 40 Park Drive, #206
Chesterfield, MO 63005

Hoyt Kesterson
Consultant
7625 West Villa Rita Drive
Glendale, AZ 85308

Larry Kreiser
Chair and Professor
Department of Accounting and Business Law
Cleveland State University
Department of Accounting
Cleveland, OH 44115-2214

Darren Lacey
Executive Director
Johns Hopkins University Information Security Institute
3400 N. Charles Street,
Wyman Building, 4th Floor
Baltimore, MD 21218

Thomas Lenahan
Professor of Criminal Justice
Herkimer County Community College
100 Reservoir Road
Herkimer, NY 13350

Fran Linhart
Director of Certification Programs
CompTIA
1815 South Meyers Road
Suite 300
Oakbrook Terrace, IL 60181-5228

Jim Litchko
President
Litchko & Associates
4604 Saul Road
Kensington, MD 20895

Kenneth Loisch
Information Security Manager
Unilever US
55 Merritt Boulevard
Bridgeport, CT 06611

Matt Luallen
Cybersecurity Engineer
Argonne National Laboratory
9700 S. Cass Avenue
Building 222/C221
Argonne, IL 60439

Kris Madura
Security Program Manager
CompTIA
1815 South Meyers Road
Suite 300
Oakbrook Terrace, IL 60181-5228

***Shirley Malia**
Cybersecurity Workforce Consultant
17100 Quarter Horse Way
Olney, MD 20832

Daniel Manson
Department Chair and Professor
Computer Information Systems
California State Polytechnic University, Pomona
3801 West Temple Avenue
Pomona, CA 92886

Randy Marchany
Director
Computer & Network Defense Initiative
Virginia Tech
3210 Torgersen Hall
Blacksburg, VA 24060

Ted Mims
Chair
Computer Science Department
University of Illinois at Springfield
PO Box 19243
Springfield, IL 62794-9243

Keith Morneau
Program Head
Information Systems Technology
Northern Virginia Community College
8333 Little River Turnpike
Annandale, VA 22003

William Oblitey
Professor and Co-Director
Center for Information Assurance
Indiana University of Pennsylvania
319 Stright Hall
210 South Tenth Street
Indiana, PA 15705-1087

Susan Ogar
Director of Product Marketing
Thomson-Course Technology
25 Thomson Place
Boston, MA 02210

Susan Older
Assistant Professor
Center for Systems Assurance
Department of Electrical Engineering
and Computer Science
Syracuse University
CST 2-177
Syracuse, NY 13244

Anthony Passaniti
Corporate Security Officer
Swiss Re Americans Holding Corporation
175 King Street
Armonk, NY 10530

Amelia Phillips
Faculty
Department of Computer Science
Highline Community College
2400 S. 240th Street
PO Box 98000 MS 15-1
Des Moines, WA 98198

Will Pitkin
Acquisitions Editor
Thomson-Course Technology
25 Thomson Place
Boston, MA 02210

Michael Porter
Assistant Professor of Computer
Information Systems
Sinclair Community College
444 West Third Street
Dayton, OH 45402-1460

Marsha Powell
Professor and Chair
Department of Computer Forensics and
Computer Information Systems
Tompkins-Cortland Community College
170 North Street
Dryden, NY 13053

David Ray
Instructor
Jones County Junior College
900 South Court Street
Ellisville, MS 39437

BEST COPY AVAILABLE

133

Jeff Recor
President
Olympus Security Group
1028 Bloomview Circle
Rochester, MI 48307

Hart Rossman
Technical Director
Secure Business Solutions Group
Science Applications International
Corporation (SAIC)
1710 SAIC Drive
Mailstrop T3-5-3
McLean, VA 22102

Julie Ryan
Assistant Professor of Engineering
Management and Systems Engineering
George Washington University
School of Engineering and Applied Science
1776 G Street NW, #110
Washington, DC 20052

John Sabo
Manager
Security, Trust and Privacy Initiatives
Computer Associates
2291 Wood Oak Drive
Herndon, VA 20171

***Peter Saflund**
Associate Director
National Workforce Center for Emerging
Technologies
Bellevue Community College
3000 Landerhold Circle, SE
N-258
Bellevue, WA 98007-6484

Jason Sakos
Marketing Manager
Thomson-Course Technology
25 Thomson Place
Boston, MA 02210

***John Sands**
Professor of Information Technology
Moraine Valley Community College
10900 S 88th Avenue
Palos Hills, IL 60465

Raemarie Schmidt
Supervisory
Computer Crime Specialist
National White Collar Crime Center
1000 Technology Drive
Suite 2130
Fairmont, WV 98027

***Corey Schou**
Professor and Associate Dean of Information
Systems
Director of the National Information
Assurance Training and Education Center
Idaho State University
Box 4043
Pocatello, ID 83205-4043

Sujeet Shenoi
Oliphant Professor of Computer Science
University of Tulsa
Center for Information Security
600 S. College Avenue
Tulsa, OK 74104

Judson Slusser
Senior Vice President
Research and Development
ProsoftTraining
2333 North Broadway
Santa Ana, CA 92706

Ben Smith
Subject Matter Expert, Security
Microsoft Corporation
One Microsoft Way
118/2405
Redmond, WA 98052

Tracey Souther
Chair
Department of Networking Technologies
Forsyth Technical Community College
2100 Silas Creek Parkway
Winston-Salem, NC 27103

Erich Spengler
Professor of Information Technology
Moraine Valley Community College
10900 S. 88th Avenue
Palos Hills, IL 60465

David Strothcamp
Information Technology Audit Manager
Cleveland Clinic Health System
9500 Euclid Avenue
Mail Code CC30
Cleveland, OH 44095

Jonathan Thomson
Central IT Director
Allied Domecq PLC
388 Riverside Avenue
Westport, CT 06880

Craig Tidwell
Program Manager
Network and Electronic Technologies
Seminole Community College
2505 Lockwood Boulevard
Oviedo, FL 32765

Mike Wenstrom
Education Program Manager
Cisco Systems, Inc.
Critical Infrastructure Assurance Group
12515 Research Boulevard
Building 2
Austin, TX 78759

Gregory White
Technical Director
Center for Infrastructure Assurance and Security
Associate Professor of Information Systems
University of Texas at San Antonio
6900 North Loop 1604 West
San Antonio, TX 78249-0630

Bob Williams
Director
Information Technology Education Center of Florida
Daytona Beach Community College
1200 W. International Speedway Boulevard
Daytona Beach, FL 32120-2811

***Marie Wright**
Professor of Management Information Systems
Western Connecticut State University
MIS Department
181 White Street
Danbury, CT 06810

Alec Yasinsac
Assistant Professor of Computer Science
Florida State University
Computer Science Department
Tallahassee, FL 32306-4530

Workshop Leadership
*Steering Committee Member

BEST COPY AVAILABLE

National Science Foundation Participants

National Science Foundation
4201 Wilson Boulevard
Arlington, VA 22230
www.nsf.gov

Office of the Deputy Director
Room: 1205N **Phone: (703) 292-8001**
Joseph Bordogna, Deputy Director

Directorate for Education & Human Resources
Room: 805N **Phone: (703) 292-8600**
Judith A. Ramaley, Assistant Director

Division of Undergraduate Education
Room: 835 **Phone: (703) 292-8670**
Celeste Carter, Program Director
Stephanie Crisp, NSF/Phi Theta Kappa Summer Intern
Corby Hovis, Program Director
Duncan McBride, Lead Program Director
Abe Nisanci, Program Director
Janeth Randall, NSF/Phi Theta Kappa Summer Intern
Melissa Squillaro, Science Education Analyst
Rich Taber, Corporate and Foundation Relations Specialist
Elizabeth Teles, Acting Division Director and ATE Lead Program Director
Sheila Veney, ATE Lead Program Assistant

Division of Elementary, Secondary, and Information Education
Room: 885 **Phone: (703) 292-8628**
Gerhard Salinger, ATE Lead Program Director

Division of Information Services
Room: 455S **Phone: (703) 292-8150**
Arthur Saenz, Computer Specialist

American Association of Community College Participants

American Association of Community Colleges
One Dupont Circle, NW
Suite 410
Washington, DC 20036
(202) 728-0200
www.aacc.nche.edu

George R. Boggs, President and CEO

Lynn Barnett, Vice President for Academic, Student and Community Development

Margaret Rivera, Vice President for Membership and Information Services

Jeff Mills, Internet Manager

Ellen Hause, Program Associate for Academic, Student and Community Development

136

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

NOTICE

Reproduction Basis

[X] This document is covered by a signed "Reproduction Release (Blanket)" form (on file within the ERIC system), encompassing all or classes of documents from its source organization and, therefore, does not require a "Specific Document" Release form.

[ ] This document is Federally-funded, or carries its own permission to reproduce, or is otherwise in the public domain and, therefore, may be reproduced by ERIC without a signed Reproduction Release form (either "Specific Document" or "Blanket").